Synopse Entwürfe IT-Sicherheitsgesetz

Stand 21.12.2014

	Entwurf 18.8.2014[1]	**Entwurf 6.11.2014 12:43[2]**	**Beschluss Kabinett 17.12.1014[3]**
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)[4]			
§ 1 Bundesamt für Sicherheit in der Informationstechnik			
Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.	Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als nationale Informationssicherheitsbehörde. Es untersteht als Bundesoberbehörde dem Bundesministerium des Innern.	Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.	*Unverändert zum Entwurf vom 6.11.2014*
§ 2 Begriffsbestimmungen			
… *neu*	… (10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind die durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmten Einrichtungen, Anlagen oder Teile davon in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und	… (10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemein-	… (10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die 3. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 4. von hoher Bedeutung für das Funktionieren des Gemein-

[1] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile
[2] https://netzpolitik.org/wp-upload/141104-Anlage-Referentenentwurf-IT-Sicherheitsgesetz-final.pdf
[3] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile
[4] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 3 Abs. 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)

	durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten würden. Kommunikationstechnik im Sinne des Absatzes 3 Satz 1 und 2 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.	wesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt. Kommunikationstechnik im Sinne des Absatzes 3 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.	wesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.
neu	(11) Betreiber Kritischer Infrastrukturen im Sinne dieses Gesetzes sind alle Unternehmen, die Kritische Infrastrukturen betreiben, mit Ausnahme solcher Unternehmen, die Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36) sind. Ein Unternehmen, das sich darauf beruft, Kleinstunternehmen im Sinne der vorgenannten Empfehlung der Kommission zu sein, hat dem Bundesamt auf dessen Verlangen das Vorliegen der dafür erforderlichen Voraussetzungen auf geeignete Weise nachzuweisen.	*Verschoben nach „§ 8c Anwendungsbereich*"	

§ 3 Aufgaben des Bundesamtes			
(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: … 2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist; … 15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der kritischen Informationsinfrastrukturen im Verbund mit der Privatwirtschaft.	(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: … 2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für <u>Dritte</u>, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist; … 15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der <u>Sicherheit der Informationstechnik Kritischer Infrastrukturen</u> im Verbund mit der Privatwirtschaft; 16. Zentrale Stelle im Bereich der Sicherheit in der Informationstechnik bei der Zusammenarbeit mit den zuständigen Stellen im Ausland.	(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: … 2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für <u>Dritte</u>, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist; … 15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der <u>Sicherheit der Informationstechnik Kritischer Infrastrukturen</u> im Verbund mit der Privatwirtschaft; 16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland;	(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr: … 2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben ~~oder~~[5] erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist; … 15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der <u>Sicherheit der Informationstechnik Kritischer Infrastrukturen</u> im Verbund mit der Privatwirtschaft; 16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen

[5] Das Wort „oder" nicht zu streichen ist offensichtlich ein redaktionelles Versehen

	…	17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. …	Stellen im Ausland<u>, unbeschadet besonderer Zuständigkeiten anderer Stellen</u>; 17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. …
neu	(3) Das Bundesamt nimmt als zentrale Stelle für die Sicherheit der Informationstechnik Kritischer Infrastrukturen die Aufgaben nach §§ 8a und 8b wahr. Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.	(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.	*Unverändert zum Entwurf vom 6.11.2014*
§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik	**§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik <u>des Bundes</u>**		
…	**…**		
§ 7 Warnungen			
(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen an die betroffenen Kreise oder die Öffentlichkeit weitergeben oder Sicherheitsmaßnahmen sowie den Ein-	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen <u>und im Falle des unberechtigten Abflusses von Daten</u> an die betroffenen Kreise oder die Öffentlichkeit weitergeben oder Sicherheitsmaßnahmen	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt 1) die folgenden Warnungen an die Öffentlichkeit oder an die betroffene Kreise richten: a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt 1) die folgenden Warnungen an die Öffentlichkeit oder an die betroffene Kreise richten: a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten

satz bestimmter Sicherheitsprodukte empfehlen. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.	sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Das Bundesamt kann sich bei der Wahrnehmung der Aufgaben nach Satz 1 der Einschaltung Dritter bedienen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.	b) Warnungen vor Schadprogrammen, c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten. 2) Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Das Bundesamt kann sich bei der Wahrnehmung der Aufgaben nach Satz 1 der Einschaltung Dritter bedienen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere	b) Warnungen vor Schadprogrammen und c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten. 2) Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere

		Zuverlässigkeit des Empfängers sein.	Zuverlässigkeit des Empfängers sein.
neu	**§ 7a Untersuchung der IT-Sicherheit**		**§ 7a Untersuchung der Sicherheit in der Informationstechnik**
neu	(1) Das Bundesamt darf zur Wahrnehmung seiner Aufgaben nach § 3 Absatz 1 Nummer 1 und § 3 Absatz 3 informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich dazu aller geeigneten technischen Mittel sowie der Unterstützung Dritter bedienen.	(1) Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung Dritter bedienen.	(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.
	(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden. Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 2 und 3 ist entsprechend anzuwenden.	(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden.	(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zu den in Absatz 1 Satz 1 genannten Zwecken genutzt werden. Soweit erforderlich darf das Bundesamt seine Erkenntnisse weitergeben und veröffentlichen. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

		(3) Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten informationstechnischen Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden."	*entfällt*
§ 8 Vorgaben des Bundesamtes			
(1) Das Bundesamt kann Mindeststandards für die Sicherung der Informationstechnik des Bundes festlegen. Das Bundesministerium des Innern kann nach Zustimmung des Rats der IT-Beauftragten der Bundesregierung die nach Satz 1 festgelegten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Soweit in einer allgemeinen Verwaltungsvorschrift Sicherheitsvorgaben des Bundesamtes für ressortübergreifende Netze sowie die für den Schutzbedarf des jeweiligen Netzes notwendigen und von den Nutzern des Netzes umzusetzenden Sicherheitsanforderungen enthalten sind, werden diese Inhalte im Benehmen mit dem Rat der IT-Beauftragten der Bundesregierung festgelegt. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane	(1) Das Bundesamt legt verbindliche Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest und berät die Bundesbehörden auf Ersuchen bei der Umsetzung und Einhaltung dieser Mindeststandards. Das Bundesministerium des Innern erlässt im Benehmen mit dem Rat der IT-Beauftragten der Ressorts die nach Satz 1 festgelegten Anforderungen als allgemeine Verwaltungsvorschriften. Das Bundesamt kann eine Überprüfung der Einhaltung der nach Satz 1 festgelegten Anforderungen in der Einrichtung durchführen. Diese ist verpflichtet, das Bundesamt und seine Beauftragten hierbei zu unterstützen. Vom Bundesamt festgestellte Mängel bei der Umsetzung dieser Anforderungen sind innerhalb einer vom Bundesamt festgelegten angemessenen Frist zu beheben. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfas-	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*

haben die Vorschriften nach diesem Absatz empfehlenden Charakter.	sungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.		
neu	**§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen**		
neu	(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen und sonstige Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.	(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.	(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
neu	(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Auf-	(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt im Benehmen mit dem Bundesamt für Be-	(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu

	sichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe auf Antrag an, wenn diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die vom Bundesamt anerkannten branchenspezifischen Sicherheitsstandards konkretisieren die organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1.	völkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.	gewährleisten. Die Feststellung erfolgt 1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.
neu	(3) Zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1 haben die Betreiber Kritischer Infrastrukturen mindestens alle zwei Jahre die Erfüllung der Anforderungen auf geeignete Weise nachzuweisen. Hierfür übermitteln sie dem Bundesamt mindestens alle zwei Jahre eine Aufstellung der zu diesem Zweck durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln eine Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen. Bei Sicherheitsmängeln kann das Bundesamt deren unverzügliche Beseitigung verlangen.	(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.	(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Neu	(4) Auf Betreiber Kritischer Infrastrukturen finden die Absätze 1 bis 3 keine Anwendung, soweit diese ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Die Vorschriften des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958), bleiben unberührt. Satz 1 gilt für Betreiber Kritischer Infrastrukturen, für die aus oder auf Grund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Anforderungen im Sinne der Absätze 1 bis 3 bestehen, entsprechend.	*Verschoben nach „§ 8c Anwendungsbereich"*	
neu	**§ 8b Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen**	**§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen**	
neu	(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse nach § 8a Absatz 1 Satz 1.	(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.	*Unverändert zum Entwurf vom 6.11.2014*
neu	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe 1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe 1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen,	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe 1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu

	wesentlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten, 2. in Zusammenarbeit mit den zuständigen Bundesbehörden die potentiellen Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu analysieren, 3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich fortzuschreiben und 4. die Betreiber Kritischer Infrastrukturen, die zuständigen Aufsichtsbehörden sowie die sonst zuständigen Bundesbehörden über sie betreffende Informationen nach den Nummern 1 bis 3 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.	insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten, 2. die potentiellen Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Bundesbehörden zu analysieren, 3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und 4. die Betreiber Kritischer Infrastrukturen, die zuständigen Aufsichtsbehörden sowie die sonst zuständigen Bundesbehörden über sie betreffende Informationen nach den Nummern 1 bis 3 und die in Erfahrung gebrachten Zusammenhänge unverzüglich zu unterrichten.	sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise, 2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungs- und Katastrophenschutz zu analysieren, 3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und 4. unverzüglich a. die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen nach den Nummern 1 bis 3, b. die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie

			c. die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 zu unterrichten.
neu	(3) Um bei Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse Kritischer Infrastrukturen eine unverzügliche Information betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten, sind dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 für den Aufbau der Kommunikationsstrukturen nach § 3 Absatz 1 Nummer 15 Warn- und Alarmierungskontakte zu benennen. Der Betreiber hat sicherzustellen, dass er hierüber jederzeit erreichbar ist. Die Unterrichtung durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt dorthin.	(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle als zuständigen Empfangspunkt im Rahmen der Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu nennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Das Bundesamt übermittelt die Informationen nach Absatz 2 Nummer 4 an diese Kontaktstelle.	(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.
neu	(4) Betreiber Kritischer Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 Satz 1 Beeinträchtigun-	(4) Betreiber Kritischer Infrastrukturen haben bedeutende Störungen ihrer informationstechnischen Systeme, Kompo-	(4) Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertrau-

	gen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastruktur führen können, unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu den technischen Rahmenbedingungen, insbesondere der eingesetzten und betroffenen Informationstechnik sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nicht erforderlich.	nenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt hat.	lichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.
neu	(5) Führt eine Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder zu einer Beeinträchtigung der Kritischen Infrastruktur, ist dies unverzüglich durch den Betreiber der Kritischen Infrastruktur über die Warn- und Alarmierungskontakte nach Absatz 3 Satz 1 unter Angabe der Informationen nach	*./.*	*./.*

	Absatz 4 Satz 2 sowie der Nennung des Betreibers an das Bundesamt zu melden.		
neu	(6) Zusätzlich zu den Warn- und Alarmierungskontakten nach Absatz 3 Satz 1 können alle oder ein Teil der Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, einen gemeinsamen Ansprechpartner benennen, über den der Informationsaustausch zwischen den Warn- und Alarmierungskontakten und dem Bundesamt nach Absatz 2 Nummer 4 und nach Absatz 4 erfolgt.	(5) Zusätzlich zu den Kontaktstellen nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt nach Absatz 2 Nummer 4 und nach Absatz 4 Satz 1 über die gemeinsame Ansprechstelle.	(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.
neu	(7) Auf Betreiber Kritischer Infrastrukturen finden die Absätze 3 bis 6 keine Anwendung, soweit diese ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Die Vorschriften des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958), bleiben unberührt. Für Betreiber Kritischer Infrastrukturen, für die aus oder auf Grund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Anforderungen im Sinne der Absätze 3 bis 6 bestehen, gilt Satz 1 entsprechend.	*./.*	(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

neu	*neu*	**§8c Anwendungsbereich**	
neu	*neu*	(1) Die §§ 8a und 8b finden keine Anwendung auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABI. L 124 vom 20.5.2003, S. 36).	(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.
Neu	*neu*	(2) § 8a findet keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8a erfüllen müssen.	(2) § 8a ist nicht anzuwenden auf 1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, 2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung, 3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565),

			das zuletzt durch Artikel 2 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie 4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.
neu	*neu*	(3) § 8b Absätze 3 bis 5 finden keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8b Absätze 3 bis 5 erfüllen müssen.	(3) § 8b Absatz 3 bis 5 ist nicht anzuwenden auf 1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, 2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, 3. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie 4. 4. sonstige Betreiber Kritischer Infrastrukturen, die

			auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.
neu	**§ 8c Auskunftsverlangen Dritter**	**§8d Auskunftsverlangen**	
neu	Das Bundesamt kann Dritten Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 anfallenden Informationen sowie zu den Meldungen nach § 8b Absatz 4 und 5 geben, wenn schutzwürdige Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist. In den Fällen des § 8a Absatz 3 und des § 8b Absatz 5 ist die Zustimmung des betroffenen Betreibers erforderlich. Zugang zu den Akten des Bundesamtes in Angelegenheiten nach § 8a und § 8b wird nicht gewährt.	(1) Das Bundesamt kann auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 erteilen, wenn keine schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist	(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.
neu	*Neu; letzter Satz des Abs. 1 dieses Entwurfs*	(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach § 8a und § 8b wird nur Verfahrensbeteiligten gewährt.	(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes.
§ 10 Ermächtigung zum Erlass von Rechtsverordnungen			

neu	(1) Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit durch Rechtsverordnung die Kritischen Infrastrukturen nach § 2 Absatz 10. Zugang zu Akten, die diese Verordnung betreffen, wird nicht gewährt.	(1) Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit anhand der in den jeweiligen Sektoren erbrachten Dienstleistungen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, ab welchem Schwellenwert welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."	(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung

			dieser Verordnung betreffen, wird nicht gewährt.
(1) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie durch Rechtsverordnung das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.	(2) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie durch Rechtsverordnung das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.	(2) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.	(2) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.
(2) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.	(3) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.	(3) Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen, die nicht der Zustimmung des Bundesrates bedarf, werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.	(3)[6] Für individuell zurechenbare öffentliche Leistungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Leistungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.

[6] Wird gemäß Artikel 8 dieses IT-Sicherheitsgesetzes in der Fassung des Kabinettbeschlusses vom 17.12.204 zum 14.8.2016 aufgehoben

neu	**§ 13 Berichtspflicht des Bundesamtes**	***§ 13 Berichtpflichten***	
neu	(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.	*Unverändert zum Entwurf vom 18.8.2014*	*Unverändert zum Entwurf vom 18.8.2014*
neu	(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern über Gefahren für die Sicherheit der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.	*Unverändert zum Entwurf vom 18.8.2014*	*Unverändert zum Entwurf vom 18.8.2014*
Telemediengesetz (TMG)[7]			
§ 13 Pflichten des Diensteanbieters			
… *neu*	… (7) Diensteanbieter im Sinne von § 7 Absatz 1 und § 10 Absatz 1 haben , soweit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch die erforderlichen technischen und organisatorischen Vorkehrungen sicherzustellen, dass ein Zugriff auf die Telekommunikations- und Datenverarbeitungssysteme nur für Berechtigte möglich ist. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichti-	… (7) Diensteanbieter im Sinne von § 7 Absatz 1, § 8 Absatz 1, § 9 und § 10 Absatz 1 haben, soweit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf ihre Telekommunikations- und Datenverarbeitungssysteme möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und Störungen, auch soweit sie durch äußere Angriffe	… (7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass 1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und 2. diese

[7] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692)

	gen. Bei personalisierten Telemediendiensten ist den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten.	bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen."	a. gegen Verletzungen des Schutzes personenbezogener Daten und b. gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.
(7) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.	(8) Der Diensteanbieter hat dem Nutzer nach Maßgabe von § 34 des Bundesdatenschutzgesetzes auf Verlangen Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten zu erteilen. Die Auskunft kann auf Verlangen des Nutzers auch elektronisch erteilt werden.	*Unverändert zum Entwurf vom 18.8.2014*	*Unverändert zum Entwurf vom 18.8.2014*
§ 15 Nutzungsdaten			
… *neu*	… (9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend.	**…** (9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum [Erkennen,] Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Eine Verwendung der Daten für andere Zwecke ist unzulässig. Störungen im Sinne des Satz 1 sind nur solche Einwirkungen auf die technischen Einrichtungen,	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*

		bei denen eine Beeinträchtigung für die Verfügbarkeit, Vertraulichkeit oder Integrität der informationsverarbeitenden Systeme des Diensteanbieters selbst oder der Nutzerinnen und Nutzer des Telemedienangebotes droht. Werden die Nutzungsdaten für diesen Zweck nicht mehr benötigt, sind diese unverzüglich, spätestens aber nach 6 Monaten zu löschen. Der betroffene Nutzer ist über die Erhebung und Verwendung der Nutzungsdaten zu unterrichten.	
§ 16 Bußgeldvorschriften			
… (2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig … 3. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt, …	*unverändert*	… (2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig … 3. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 <u>oder Abs. 7 Satz 1</u> über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt, …	… (2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig … 3. einer Vorschrift des § 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5 <u>oder Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a</u> über eine dort genannte Pflicht zur Sicherstellung zuwiderhandelt, …

Telekommunikationsgesetz (TKG)[8]			
§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten			
(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. **...**	(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen, einschließlich der Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. …	(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations-und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.	*Unverändert zum Entwurf vom 6.11.2014*
§ 109 Technische Schutzmaßnahmen			
… (2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen 1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -	… (2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen 1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und	*Unverändert zum Entwurf vom 18.8.2014*	… (2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen 1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und

[8] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 22 des Gesetzes vom 25. Juli 2014 (BGBl. I S. 1266)

diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und 2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten. Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 11 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.	-diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und 2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten. Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Maßnahmen nach Satz 2 müssen den Stand der Technik berücksichtigen. Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 11 Absatz 1		-diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und 2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten. Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Bei Maßnahmen nach Satz 2 ist der Stand der Technik zu berücksichtigen. Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder –dienste steht. § 11 Absatz 1

	des Bundesdatenschutzgesetzes gilt entsprechend.		des Bundesdatenschutzgesetzes gilt entsprechend.
… (4) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht, 1. welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden, 2. von welchen Gefährdungen auszugehen ist und 3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind. Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden,	./.	./.	… (4) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht, 1. welches öffentliche Telekommunikationsnetz betrieben und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden, 2. von welchen Gefährdungen auszugehen ist und 3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind. Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann nach der Bereitstellung des Telekommunikationsdienstes von der Bundesnetzagentur verpflichtet werden,

das Sicherheitskonzept vorzulegen. Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Satz 2 oder 3 Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Bundesnetzagentur kann die Umsetzung des Sicherheitskonzeptes überprüfen.			das Sicherheitskonzept vorzulegen. Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Satz 2 oder 3 Verpflichtete das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen.
(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur eine Sicherheitsverletzung einschließlich Störungen von Telekommunikationsnetzen oder -diensten unverzüglich mitzuteilen, sofern hierdurch beträchtliche Auswirkungen auf den Betrieb der Telekom-	(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu beträchtlichen Sicherheitsverletzungen einschließlich Störungen der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations-	(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und –diensten mitzuteilen, die zu beträchtlichen Sicherheitsverletzungen einschließlich Störungen, die zu einer Einschränkung der Verfüg-	(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die 1. zu beträchtlichen Sicherheitsverletzungen führen oder 2. zu beträchtlichen Sicherheitsverletzungen führen können.

munikationsnetze oder das Erbringen von Telekommunikationsdiensten entstehen. Die Bundesnetzagentur kann von dem nach Satz 1 Verpflichteten einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Erforderlichenfalls unterrichtet die Bundesnetzagentur das Bundesamt für Sicherheit in der Informationstechnik, die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit informieren oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. Die Bundesnetzagentur legt der Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen vor.	und Datenverarbeitungssysteme der Nutzer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, der Bundesnetzagentur unverzüglich mitzuteilen. Sofern es bereits zu einer Sicherheitsverletzung im Sinne von Satz 1 gekommen ist, durch die beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten entstehen, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um IT-Sicherheitsvorfälle handelt, sind die eingegangenen Meldungen sowie Informationen zu den ergriffenen Abhilfemaßnahmen von der Bundesnetzagentur unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiterzuleiten. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit informieren oder die nach Satz 1 Verpflichteten zu	barkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Für den Inhalt der Mitteilung an die Bundesnetzagentur gilt § 8b Absatz 4 Satz 2 des BSI-Gesetzes entsprechend. Kommt es zu einer Sicherheitsverletzung im Sinne von Satz 1, die beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten hat, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen können, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die	Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen.

	dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. Die Bundesnetzagentur legt der Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen vor.	Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen vor."	Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. § 8d des BSI-Gesetzes gilt entsprechend. Die Bundesnetzagentur legt der Europäischen Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.
(6) Die Bundesnetzagentur erstellt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. Sie	(6) Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und im Benehmen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absät-	*Unverändert zum Entwurf vom 18.8.2014*	(6) Die Bundesnetzagentur erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten als Grundlage für das Sicherheitskonzept nach Absatz 4 und für die zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen nach den Absätzen 1 und 2. Sie

gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht.	zen 1 und 2. Sie gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht.		gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht.
neu	(7) Über aufgedeckte Mängel bei der Erfüllung der maßgeblichen IT-Sicherheitsanforderungen sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.	*Redaktionelles Versehen, dass zur Doppelung von Abs. 7 führte. Wird in im Entwurf vom 6.11.2014 als Abs. 8 eingefügt.*	*./.*
(7) Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 3 erfüllt sind. Der nach Satz 1 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur zu übermitteln. Er trägt die Kosten dieser Überprüfung.	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*

neu	*Der in diesem Entwurf als doppelter Abs. 7 eingefügte Absatz wird im Entwurf vom 6.11.2014 als Abs. 8 eingefügt*	(8) Über aufgedeckte Mängel bei der Erfüllung der maßgeblichen IT-Sicherheitsanforderungen sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.	(8) Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.
§ 109a Datensicherheit	**§109a Daten- und Informationssicherheit**		
… *neu*	… (4) Werden Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, sind diese vom Diensteanbieter unverzüglich zu benachrichtigen. Soweit technisch möglich und zumutbar, müssen die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hingewiesen werden, mit deren Hilfe die Nutzer Störungen, die von ihren Datenverarbeitungssystemen ausgehen, erkennen und beseitigen können.	… (4) Werden <u>dem Diensteanbieter</u> Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die auf angemessene, wirksame und zugängliche technische Mittel hin mit denen sie diese Störungen erkennen und beseitigen können.	… (4) Werden <u>dem Diensteanbieter nach Absatz 1</u> Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können.
(4) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des	(5) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des	*Unverändert zum Entwurf vom 18.8.2014*	*Unverändert zum Entwurf vom 18.8.2014*

Schutzes personenbezogener Daten erforderlich ist.	Schutzes personenbezogener Daten erforderlich ist.		
§ 115 Kontrolle und Durchsetzung von Verpflichtungen			
… (3) Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen. …	… (3) Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen. Dies gilt auch dann, wenn andere Tatsachen die Annahme rechtfertigen, dass das betroffene Unternehmen nicht die erforderliche Zuverlässigkeit zur Einhaltung der Verpflichtungen des Teils 7 besitzt. …	… (3) Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen. „Dies gilt auch dann, wenn der Verpflichtete aufgrund seiner organisatorischen Struktur oder aus rechtlichen Gründen nicht die Gewähr zur Einhaltung der Verpflichtungen des Teils 7 bietet. …	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*
§ 149 Bußgeldvorschriften			
(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig … 21a entgegen § 109 Absatz 5 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht, …	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig … 21a entgegen § 109 Absatz 5 Satz 1 Nummer 1 eine Beeinträchtigung von Telekommunikationsnetzen oder -diensten, die zu einer beträchtlichen Sicherheitsverletzung führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt,

			…
Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG)[9]			
§ 11 Betrieb von Energieversorgungsnetzen			
… (1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes wird vermutet, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Die Regulierungsbehörde kann durch Festlegung im Verfahren nach § 29 Absatz 1 nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 3 treffen. **…**	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	… (1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu grundsätzlich im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Soweit der Bereich der Sicherheit in der Informationstechnik betroffen ist, ist Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik herzustellen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Anforderungen. § 8a Absatz 3 des BSI-Gesetzes gilt entsprechend. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Si-	… (1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und

[9] Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), zuletzt geändert durch Art. 6 des Gesetzes vom 21. Juli 2014 (BGBl. I S. 1066)

		cherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen Format, Inhalt und Gestaltung der Dokumentation treffen.	Gestaltung der Dokumentation nach Satz 4 treffen. **...**
neu	*./.*	(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, zu gewährleisten. Die Bundesnetzagentur erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Soweit die Sicherheitsanforderungen den	(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom … [einsetzen: Ausfertigungsdatum dieses Gesetzes und Fundstelle] geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen

		Bereich der Sicherheit in der Informationstechnik betreffen, ist ein Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik herzustellen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Anforderungen. Ein angemessener Schutz des Betriebs von Energieanlangen liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation treffen.	Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes haben Vorgaben auf Grund des Atomgesetzes Vorrang. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 6 treffen.
Neu	*./.*	(1c) Betreiber von Energieversorgungsnetzen und Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 des Gesetzes über das Bundesamt für Sicherheit in	(1c) Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt

		der Informationstechnik als Kritische Infrastruktur bestimmt wurden, haben Beeinträchtigungen von Telekommunikations- und elektronischen Datenverarbeitungssystemen, die zu einer Gefährdung oder Störung der Sicherheit oder Zuverlässigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden. Für den Inhalt der Meldung gilt § 8b Absatz 4 Satz 2 des BSI-Gesetzes entsprechend. Die Meldung muss neben Angaben zum Betreiber auch Angaben zu dem eingesetzten und betroffenen Telekommunikations- oder elektronischen Datenverarbeitungssystems enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet die Meldungen unverzüglich an die Bundesnetzagentur weiter. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstech-	wurden, haben dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kennt-

		nik sowie zu den Akten der Bundesnetzagentur nach dieser Vorschrift wird nicht gewährt."	nis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach den §§ 11a bis 11c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8d Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden.
§ 21e Allgemeine Anforderungen an Messsysteme zur Erfassung elektrischer Energie			
… (5) Messsysteme, die den Anforderungen der Absätze 2 und 4 nicht entsprechen, dürfen noch bis zum 31. Dezember 2014 eingebaut und bis zu acht Jahre ab Einbau genutzt werden, 1. wenn ihre Nutzung nicht mit unverhältnismäßigen Gefahren verbunden ist und 2. solange eine schriftliche Zustimmung des Anschlussnutzers zum Einbau und zur Nutzung eines Messsystems besteht, die er in der Kenntnis erteilt hat, dass das Messsystem nicht den Anforderungen der Absätze 2 und 4 entspricht. Der Anschlussnutzer kann die Zustimmung widerrufen. Solange die Voraussetzungen des Satzes 1 vorliegen, bestehen die Pflichten nach § 21c Absatz 1	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	… (5) Messsysteme, die den Anforderungen der Absätze 2 und 4 nicht entsprechen, dürfen noch <u>bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt</u>, mindestens jedoch bis zum 31. Dezember 201<u>5</u> eingebaut und bis zu acht Jahre ab Einbau genutzt werden, 3. wenn ihre Nutzung nicht mit unverhältnismäßigen Gefahren verbunden ist und 4. solange eine schriftliche Zustimmung des Anschlussnutzers zum Einbau und zur Nutzung eines Messsystems besteht, die er in der Kenntnis erteilt hat, dass das Messsystem nicht den Anforderungen der Absätze 2 und

und auf Grund einer nach § 21c Absatz 5 erlassenen Rechtsverordnung nicht. Näheres kann durch Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt werden			4 entspricht. Der Anschlussnutzer kann die Zustimmung widerrufen. Solange die Voraussetzungen des Satzes 1 vorliegen, bestehen die Pflichten nach § 21c Absatz 1 und auf Grund einer nach § 21c Absatz 5 erlassenen Rechtsverordnung nicht. ~~Näheres kann durch Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt werden~~
§ 21f Messeinrichtungen für Gas			
… (2) Bestandsgeräte, die den Anforderungen eines speziellen Schutzprofils nicht genügen, können noch bis zum 31. Dezember 2014 eingebaut werden und dürfen bis zum nächsten Ablauf der bestehenden Eichgültigkeit weiter genutzt werden, es sei denn, sie wären zuvor auf Grund eines Einbaus nach § 21c auszutauschen oder ihre Weiterbenutzung ist mit unverhältnismäßigen Gefahren verbunden. Näheres kann durch Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt werden.	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	… (2) Bestandsgeräte, die den Anforderungen eines speziellen Schutzprofils nicht genügen, können noch <u>bis zum Zeitpunkt, den eine Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt,</u> <u>mindestens jedoch</u> bis zum 31. Dezember 201<u>5</u> eingebaut werden und dürfen bis zum nächsten Ablauf der bestehenden Eichgültigkeit weiter genutzt werden, es sei denn, sie wären zuvor auf Grund eines Einbaus nach § 21c auszutauschen oder ihre Weiterbenutzung ist mit unverhältnismäßigen Gefahren verbunden. ~~Näheres kann durch Rechtsverordnung nach § 21i Absatz 1 Nummer 11 bestimmt werden.~~
§ 21i Rechtsverordnungen			

(1) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates … 11. den Bestandsschutz nach § 21e Absatz 5 und § 21f Absatz 2 inhaltlich und zeitlich näher zu bestimmen und damit gegebenenfalls auch eine Differenzierung nach Gruppen und eine Verlängerung der genannten Frist vorzunehmen; …	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	(1) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates … 11. den Bestandsschutz nach § 21e Absatz 5 und § 21f Absatz 2 inhaltlich und zeitlich näher zu bestimmen und damit gegebenenfalls auch eine Differenzierung nach Gruppen ~~und eine Verlängerung der genannten Frist~~ vorzunehmen; …
§ 59 Organisation			
(1) Die Entscheidungen der Bundesnetzagentur nach diesem Gesetz werden von den Beschlusskammern getroffen. Satz 1 gilt nicht für die Erstellung von Katalogen von Sicherheitsanforderungen nach § 11 Absatz 1a Satz 2, Erhebung von Gebühren nach § 91, die Durchführung des Vergleichsverfahrens nach § 21 Absatz 3, die Datenerhebung zur Erfüllung von Berichtspflichten, Datenerhebungen zur Wahrnehmung der Aufgaben nach § 54a Absatz 2, Entscheidungen im Zusammenhang mit dem Ausbau bidirektionaler Gasflüsse nach § 54a Absatz 2 in Verbindung mit Artikel 7 und 6 Absatz 5 bis 7 der Verordnung (EU) Nr. 994/2010 sowie Festlegungen gemäß § 54a	*Unverändert bezgl. der derzeit gelten Fassung des Gesetzes*	(1) Die Entscheidungen der Bundesnetzagentur nach diesem Gesetz werden von den Beschlusskammern getroffen. Satz 1 gilt nicht für die Erstellung <u>und Überprüfung</u> von Katalogen von Sicherheitsanforderungen nach § 11 Absatz 1a <u>und 1b</u>, Erhebung von Gebühren nach § 91, die Durchführung des Vergleichsverfahrens nach § 21 Absatz 3, die Datenerhebung zur Erfüllung von Berichtspflichten, Datenerhebungen zur Wahrnehmung der Aufgaben nach § 54a Absatz 2, Entscheidungen im Zusammenhang mit dem Ausbau bidirektionaler Gasflüsse nach § 54a Absatz 2 in Verbindung mit Artikel 7 und 6 Absatz 5 bis 7 der Verordnung	*Unverändert zum Entwurf vom 6.11.2014*

Absatz 3 Satz 2 mit Ausnahme von Festlegungen zur Kostenaufteilung, Entscheidungen im Zusammenhang mit der Überwachung der Energiegroßhandelsmärkte nach § 56 Satz 1 Nummer 4 in Verbindung mit der Verordnung (EU) Nr. 1227/2011 sowie Festlegungen gemäß § 5b Absatz 1 Satz 2 und § 58a Absatz 4, Maßnahmen nach § 94, die Aufgaben nach den §§ 12a bis 12f, 15a, 17b und 17c sowie die Vorgaben zu den Netzzustands- und Netzausbauberichten nach § 14 Absatz 1a Satz 5, Genehmigungen nach § 13a Absatz 2 und § 13c Absatz 1 sowie Festlegungen nach § 13b Absatz 3 und § 13c Absatz 3. Die Beschlusskammern werden nach Bestimmung des Bundesministeriums für Wirtschaft und Technologie gebildet.		(EU) Nr. 994/2010 sowie Festlegungen gemäß § 54a Absatz 3 Satz 2 mit Ausnahme von Festlegungen zur Kostenaufteilung, Entscheidungen im Zusammenhang mit der Überwachung der Energiegroßhandelsmärkte nach § 56 Satz 1 Nummer 4 in Verbindung mit der Verordnung (EU) Nr. 1227/2011 sowie Festlegungen gemäß § 5b Absatz 1 Satz 2 und § 58a Absatz 4, Maßnahmen nach § 94, die Aufgaben nach den §§ 12a bis 12f, 15a, 17b und 17c sowie die Vorgaben zu den Netzzustands- und Netzausbauberichten nach § 14 Absatz 1a Satz 5, Genehmigungen nach § 13a Absatz 2 und § 13c Absatz 1 sowie Festlegungen nach § 13b Absatz 3 und § 13c Absatz 3. Die Beschlusskammern werden nach Bestimmung des Bundesministeriums für Wirtschaft und Technologie gebildet.	
Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) (Bundeskriminalamtgesetz - BKAG)[10]			
§ 4 Strafverfolgung			
(1) Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr …	(1) Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr …	(1) Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr …	*Wie Entwurf vom 18.8.2014*

[10] Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Artikel 3 iVm Artikel 9 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602)

5. in den Fällen von Straftaten nach § 303b des Strafgesetzbuches, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen a) die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder b) sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, richtet. …	5. in den Fällen von Straftaten nach den §§ 202a, 202b, 202c, 263a, 303a und 303b des Strafgesetzbuches, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen a) die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder b) Behörden oder Einrichtungen des Bundes oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, richtet. …	5. in den Fällen von Straftaten nach den § 303b des Strafgesetzbuches, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen a) die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder b) Behörden oder Einrichtungen des Bundes oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, richtet. …	
Außenwirtschaftsgesetz (AWG)[11]			
§ 5 Gegenstand von Beschränkungen			
… (3) Beschränkungen oder Handlungspflichten nach § 4 Absatz 1 Nummer 1 können insbesondere angeordnet werden in Bezug auf	… (3) Beschränkungen oder Handlungspflichten nach § 4 Absatz 1 Nummer 1 können insbesondere angeordnet werden in Bezug auf	*Unverändertes derzeit geltendes Gesetz, da der Entwurf vom 6.11.2014 das AWG nicht ändert*	*Unverändertes derzeit geltendes Gesetz, da die Fassung des Kabinettbeschlusses vom 17.12.2014 das AWG nicht ändert*

[11] Außenwirtschaftsgesetz vom 6. Juni 2013 (BGBl. I S. 1482)

den Erwerb inländischer Unternehmen oder von Anteilen an solchen Unternehmen durch Ausländer, um wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten, wenn die inländischen Unternehmen 1. Kriegswaffen oder andere Rüstungsgüter herstellen oder entwickeln oder 2. Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung von staatlichen Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellen oder hergestellt haben und noch über die Technologie verfügen, wenn das Gesamtprodukt mit Wissen des Unternehmens vom Bundesamt für Sicherheit in der Informationstechnik zugelassen wurde. Dies gilt insbesondere dann, wenn infolge des Erwerbs die sicherheitspolitischen Interessen der Bundesrepublik Deutschland oder die militärische Sicherheitsvorsorge gefährdet sind. …	den Erwerb inländischer Unternehmen oder von Anteilen an solchen Unternehmen durch Ausländer, um wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten, wenn die inländischen Unternehmen 1. Kriegswaffen oder andere Rüstungsgüter herstellen oder entwickeln oder 2. Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung von staatlichen Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellen oder hergestellt haben und noch über die Technologie verfügen, wenn das Gesamtprodukt mit Wissen des Unternehmens vom Bundesamt für Sicherheit in der Informationstechnik zugelassen wurde 3. mit der Umsetzung technischer oder organisatorischer Maßnahmen nach § 110 des Telekommunikationsgesetzes betraut sind oder die technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation herstellen oder vertreiben.		

	Dies gilt insbesondere dann, wenn infolge des Erwerbs die sicherheitspolitischen Interessen der Bundesrepublik Deutschland oder die militärische Sicherheitsvorsorge gefährdet sind. …		
Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)[12]			
§ 44b Meldewesen für die Sicherheit in der Informationstechnik			
neu	*./.*	*./.*	Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 und 6 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die

[12] Atomgesetz in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), zuletzt geändert durch Artikel 5 des Gesetzes vom 28. August 2013 (BGBl. I S. 3313)

			für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiter.