

[Entwurf von 2013]

[Entwurf von 2014]

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Vom ...

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

Artikel 1
Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

Das BSI-Gesetz vom 14. August 2009 (BGBl. I, S. 2821) wird wie folgt geändert:

Das BSI-Gesetz vom 14. August 2009 (BGBl. I, S. 2821) wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als nationale Informationssicherheitsbehörde. Es untersteht als Bundesoberbehörde dem Bundesministerium des Innern.“

1. Dem § 2 Absatz 9 wird folgender Absatz 10 angefügt:

2. Dem § 2 Absatz 9 werden folgende Absätze 10 und 11 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind die in der 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 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.“

„(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 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.“

(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.“

2. § 3 wird wie folgt geändert:

a. In § 3 Absatz 1 Satz 2 Nummer 2 werden die Wörter „andere Stellen“ durch das Wort „Dritte“ ersetzt.

b. Folgender Absatz 3 wird angefügt:

„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.**“

3. Die Überschrift von § 4 wird wie folgt gefasst:

„Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes“.

3. § 3 wird wie folgt geändert:

a. In Absatz 1 Satz 2 Nummer 2 werden die Wörter „andere Stellen“ durch das Wort „Dritte“ ersetzt.

b. In Absatz 1 Satz 2 Nummer 15 werden die Worte „kritischen **Informationen**“ durch die Worte „der Sicherheit der **Informationstechnik Kritischer** Infrastrukturen“ und der Punkt durch ein Semikolon ersetzt.

c. In Absatz 1 Satz 2 wird folgende Nummer 16 angefügt:

„Zentrale Stelle im Bereich der Sicherheit in der Informationstechnik bei der Zusammenarbeit mit den zuständigen Stellen im Ausland.“

d. Folgender Absatz 3 wird angefügt:

„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.**“

4. Die Überschrift von § 4 wird wie folgt gefasst:

„Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes“.

5. § 7 Absatz 1 wird wie folgt geändert:

a. In Satz 1 werden nach dem Wort „Schadprogrammen“ die Worte „und im Falle des unberechtigten Abflusses von Daten“ eingefügt.

b. Nach Satz 1 wird folgender Satz 2 eingefügt:

„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.“

c. Die bisherigen Sätze 2 und 3 werden die Sätze 3 und 4.

6. Nach § 7 wird folgender § 7a eingefügt:

„§ 7a
Untersuchung der IT-Sicherheit
„(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.“

(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."

7. § 8 Absatz 1 wird wie folgt geändert:

a. § 8 Absatz 1 Satz 1 wie folgt gefasst:

„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.“

b. § 8 Absatz 1 Sätze 2 bis 4 werden wie folgt gefasst und ein neuer Satz 5 angefügt:

„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.“

c. Der bisherige Satz 3 wird gestrichen.

d. Der bisherige Satz 4 wird Satz 6.

4. Nach § 8 werden folgende §§ 8a und 8b eingefügt:

„§ 8a Sicherheit der Informationstechnik **kritischer** Infrastrukturen

(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.

(2) Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von

8. Nach § 8 werden folgende §§ 8a, 8b und 8c eingefügt:

„§ 8a Sicherheit **in** der Informationstechnik **Kritischer** Infrastrukturen

(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.

informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen und Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt wurden.

(3) Betreiber kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards erarbeiten. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Aufsichtsbehörden 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.

(4) Betreiber kritischer Infrastrukturen haben zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1 nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 mindestens alle zwei Jahre Sicherheitsaudits durch anerkannte Auditoren durchzuführen. Sie übermitteln dem Bundesamt mindestens alle zwei Jahre eine Aufstellung der durchgeführten Sicherheitsaudits einschließlich der aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln eine Übermittlung der gesamten Ergebnisse des Sicherheitsaudits verlangen. Bei Sicherheitsmängeln kann das Bundesamt deren unverzügliche Beseitigung verlangen.

(5) Soweit aus oder auf Grund von Rechtsvorschriften des Bundes weitergehende Anforderungen an die informationstechnischen Systeme, Komponenten oder Prozesse kritischer Infrastrukturen anzuwenden sind, finden die Absätze 1 bis 4 keine Anwendung.

§ 8b

Zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Aufsichtsbehörden 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.

(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.

(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 ge-ändert 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.

§ 8b

Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(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.

Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse nach § 8a Absatz 1 Satz 1.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik 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 und die zuständigen Aufsichtsbehörden **unverzüglich über** die sie **betreffenden** Informationen nach den Nummern 1 bis 3 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik 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.

(3) Um bei **schwerwiegenden** Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse **kritischer** Infrastrukturen eine unverzügliche Information betroffener Betreiber **kritischer** Infrastrukturen zu gewährleisten, sind dem Bundesamt binnen **eines Jahres** 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 **des Bundesamtes** nach Absatz 2 Nummer 4 erfolgt dorthin.

(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.

(4) Betreiber **kritischer** Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, das heißt Beeinträchtigungen, die Auswirkungen auf die Funktionsfähigkeit der von ihnen betriebenen **kritischen** Infrastrukturen haben können, unverzüglich an das Bundesamt zu melden.

(4) Betreiber **Kritischer** Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 **Satz 1** Beeinträchtigungen 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.

(5) **Soweit aus** oder **auf Grund von** Rechtsvorschriften des Bundes bereits Anforderungen im Sinne der Absätze 3 und 4 bestehen, finden die Absätze 3 und 4 keine Anwendung. Die in den genannten

(5) **Führt** eine Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem **Ausfall** oder zu einer Beeinträchtigung der **Kritischen** Infrastruktur, ist dies

Rechtsvorschriften benannten Meldestellen oder Aufsichtsbehörden haben Meldungen zu erheblichen IT-Sicherheitsvorfällen im Sinne von Absatz 4 unverzüglich an das Bundesamt weiterzuleiten.

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.

(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.

(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.

§ 8c

Auskunftsverlangen Dritter
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."

5. § 10 wird wie folgt geändert:

a. Vor Absatz 1 wird folgender neuer Absatz 1 eingefügt:

„Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem

9. § 10 wird wie folgt geändert:

a. Vor Absatz 1 wird folgender neuer Absatz 1 eingefügt:

„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

Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, Bau und Stadtentwicklung, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit durch Rechtsverordnung die kritischen Infrastrukturen nach § 2 Absatz 10."

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."

b. Die bisherigen Absätze 1 und 2 werden die Absätze 2 und 3.

b. Die bisherigen Absätze 1 und 2 werden die Absätze 2 und 3.

6. Nach § 12 wird folgender § 13 eingefügt:

10. Nach § 12 wird folgender § 13 eingefügt:

„§ 13
Berichtspflicht des Bundesamtes
(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

„§ 13
Berichtspflicht des Bundesamtes
(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

(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 2 und 3 ist entsprechend anzuwenden".

(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."

Artikel 2

Änderung des Bundeskriminalamtgesetzes
§ 4 Absatz 1 Satz 1 Nummer 5 des Bundeskriminalamtgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 3 des Gesetzes vom 21. Juli 2012 (BGBl. I S. 1566) geändert worden ist, wird wie folgt geändert:

1. Die Angabe „§ 303b" wird durch die Wörter „den §§ 202a, 202b, 202c, 263a, 303a und 303b" ersetzt,

2. vor dem Wort „sicherheitsempfindliche" werden die Wörter „Behörden oder Einrichtungen des Bundes oder" eingefügt.

Artikel 3

Änderung des Telemediengesetzes
§ 13 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. Nach Absatz 6 wird folgender Absatz 7 eingefügt:

„Diensteanbieter haben für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien technische Vorkehrungen oder sonstige Maßnahmen zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen

Artikel 2

Änderung des Telemediengesetzes
Das Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. § 13 wird wie folgt geändert:

a. Nach Absatz 6 wird folgender Absatz 7 eingefügt:

„(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

unerlaubten Zugriff zu treffen, soweit dies technisch möglich und zumutbar ist. Dabei ist der Stand der Technik zu berücksichtigen.“

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 berücksichtigen. Bei personalisierten Telemediendiensten ist den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten.“

2. Der bisherige Absatz 7 wird Absatz 8.

b. Der bisherige Absatz 7 wird Absatz 8.

2. Nach § 15 Absatz 8 wird folgender Absatz 9 eingefügt:

„(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.“

Artikel 4 Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958) geändert worden ist, wird wie folgt geändert:

Artikel 3 Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958) geändert worden ist, wird wie folgt geändert:

1. § 100 Absatz 1 wird wie folgt gefasst:

„(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. §109 Abs.2 wird wie folgt geändert:

Nach Satz 4 wird folgender Satz 5 eingefügt:
„Maßnahmen nach Satz 2 müssen den Stand der Technik berücksichtigen.“

2. § 109 Absatz 2 wird wie folgt geändert:

a. Nach Satz 2 wird folgender Satz 3 eingefügt:
„Maßnahmen nach Satz 2 müssen den Stand der Technik berücksichtigen.“
b. Die bisherigen Sätze 3 und 4 werden Sätze 4 und 5.

3. § 109 Absatz 5 wird wie folgt gefasst:

„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- 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 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."

4. § 109 Absatz 6 wird wie folgt geändert:

Das Wort „Benehmen“ in Satz 1 wird durch „Einvernehmen“ ersetzt. Vor den Worten „dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ werden die Worte „im Benehmen mit“ eingefügt.

5. Nach § 109 Absatz 6 wird folgender Absatz 7 eingefügt:

„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.“

2. § 109a wird wie folgt geändert:

a. Die Überschrift wird wie folgt gefasst:

6. § 109a wird wie folgt geändert:

a. Die Überschrift wird wie folgt gefasst:

„§109a
Daten- und Informationssicherheit“.

b. Nach Absatz 3 wird folgender Absatz 4
eingefügt:

„Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, der Bundesnetzagentur unverzüglich mitzuteilen. Die Bundesnetzagentur unterrichtet das Bundesamt für Sicherheit in der Informationstechnik. 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.“

c. Der bisherige Absatz 4 wird Absatz 5.

„§109a
Daten- und Informationssicherheit“.

b. Nach Absatz 3 wird folgender Absatz 4
eingefügt:

„(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.“

c. Der bisherige Absatz 4 wird Absatz 5.

7. In § 115 Absatz 3 wird nach Satz 1
folgender Satz 2 eingefügt:

„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.“

Artikel 4
Änderungen des Außenwirtschaftsgesetzes

In § 5 Absatz 3 wird folgende Nummer 3
angefügt:

„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.“

Artikel 5
Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 7. Juli

1997 (BGBl. I S. 1650), das zuletzt durch Artikel 2 des SIS-II-Gesetzes vom 6. Juni 2009 (BGBl. I S. 1226) geändert worden ist, wird wie folgt geändert:

§ 4 Absatz 1 Satz 1 Nummer 5 wird wie folgt geändert:

a. Die Angabe „§ 303b“ wird durch die Wörter „den §§ 202a, 202b, 202c, 263a, 303a und 303b“ ersetzt,

b. vor dem Wort „sicherheitsempfindliche“ werden die Wörter „Behörden oder Einrichtungen des Bundes oder“ eingefügt.

Artikel 5
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Artikel 6
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.