Cyber-Sicherheitsrat Deutschland e.V.

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)300

CSRD e.V. – Georgenstraße 22 – 10117 Berlin

Deutscher Bundestag
Wolfgang Bosbach, MdB
Vorsitzender des Innenausschusses
Platz der Republik 1

11011 Berlin

Berlin, 20. April 2015

Sehr geehrter Herr Bosbach,
Lieber Herr Bosbach,

im Anhang zu diesem Schreiben erhalten Sie unsere Stellungnahme zum geplanten IT-Sicherheitsgesetz. Dies umfasst unsere Kommentierung des Entwurfs aus Dezember 2014 sowie die Kurzfassung der von uns in Auftrag gegebenen und von dem renommierten Verfassungsrechts-Experten Christoph Ahlhaus erstellte, verfassungsrechtliche Gutachten.

Ich würde mich freuen, wenn dies in Ihren Entscheidungen Berücksichtigung findet. Gerne stehe ich auch für ein Gespräch zur Verfügung.

Mit freundlichen Grüßen
Arne Schönbohm
Arne Schönbohm

Cyber-Sicherheitsrat Deutschland e.V. • Georgenstraße 22 • 10117 Berlin • Tel.: (+49)30 6796365 28 • Fax: (+49)30 6796365 29
Email: info@cybersicherheitsrat.de • www.cybersicherheitsrat.de
Präsidium: Arne Schönbohm (Präsident) • Hans-Wilhelm Dünn (Vizepräsident)
Prof. Dr. Dr. h.c. Werner Weidenfeld • Hans-Peter Kröger
Amtsgericht: Charlottenburg (Berlin) • Vereinsregisternummer: VR 31808B
Bank: Berliner Sparkasse • Konto: 190153121 • BLZ: 10050000

Cyber-Sicherheitsrat Deutschland e.V.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

Der Cyber-Sicherheitsrat Deutschland e.V. (CSRD) vertritt mit seinen Mitgliedern knapp zwei Millionen Arbeitnehmer sowie zahlreiche Bundesländer und verschiedene Institutionen. Hierzu zählen große und mittelständische Unternehmen, Betreiber kritischer Infrastrukturen sowie Experten und politische Entscheider mit Bezug zum Thema Cyber-Sicherheit. Der in Berlin ansässige Verein ist politisch neutral und hat zum Zweck Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cyber-Sicherheit zu beraten und im Kampf gegen die Cyber-Kriminalität zu stärken.

Das Bundesministerium des Innern hat am 5. März 2013 einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt und die Verbände aufgefordert, hierzu Stellung zu nehmen. Der CSRD ist dieser Aufforderung in seinem Positionspapier vom 8. März 2013 nachgekommen. Am 18. August 2014 hat das Bundesministerium einen zweiten Referentenentwurf veröffentlicht. Diesen Entwurf hat der CSRD am 24. September 2014 kommentiert. Der dritte Entwurf folgte am 04. November 2014 und wurde ebenfalls kommentiert, obwohl der Entwurf noch nicht innerhalb der Bundesregierung abgestimmt wurde. Vorliegend nimmt der CSRD Stellung zum endgültigen Entwurf vom 19. November 2014.

Zusammenfassung

- Das Gesetz betrifft KRITIS Unternehmen ab 10 Mitarbeitern und einem Jahresumsatz von mehr als 2 Mio. Euro Der damit geschaffene Aufwand ist unverhältnismäßig im Vergleich zur Bedeutung dieser Unternehmen für Wirtschaft und Gesellschaft.
- Nach heftiger Kritik soll nun die IT-Sicherheit der Bundesverwaltung ausgebaut werden. Die Anforderungen sollen jedoch weit unter denen für Unternehmen bleiben. Damit ist ersichtlich, dass der Bund das Gesetz für nicht praktikabel erachtet.
- Die reine Verbreitung von Informationen genügt nicht. Das BSI sollte vielmehr verpflichtet werden, bei Abwehr von Angriffen Beistand zu leisten.
- Die verursachende Industrie (Soft- und Hardwarehersteller) ist nach wie vor nicht Adressat des Gesetzes.
- Der geplante Erfüllungsaufwand entspricht im Wesentlichen dem Entwurf vom 18. August 2014 und ist zu knapp bemessen. Die vorgesehenen Mittel, in Höhe von 0,5 % des Haushalts des BMI, stehen in keinem Verhältnis zu den hohen Schäden durch Cyber-Kriminalität.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

1. Branchenspezifische Mindestanforderungen an die IT-Sicherheit – Der CSRD begrüßt die Einführung branchenspezifischer Mindeststandards an die IT-Sicherheit (sog. „Stand der Technik“). Jedoch ist der Anwendungsbereich des Gesetzes überzogen und unverhältnismäßig. Da das Gesetz seine Anwendung unabhängig von der Organisationsform des Betreibers Kritischer Infrastrukturen finden soll, sehen sich auch Kleinunternehmen mit mehr als 10 Mitarbeitern und einem Jahresumsatz von mehr als 2 Mio. Euro (gemäß Empfehlung 2003/361/EG der Kommission) einem enormen und nicht praktikablen Aufwand gegenüber. Dieser Aufwand überwiegt bei weitem die Bedeutung solcher Unternehmen für die Funktionsfähigkeit der Wirtschaft und Gesellschaft.
Kritisch ist auch die vorgeschlagene Umsetzungsfrist von zwei Jahren (§ 8a Abs. 1 BSI-Gesetz). Zwar ist der CSRD grundsätzlich der Ansicht, dass der Schutz von KRITIS schnell vorangetrieben werden muss. Jedoch ist zu berücksichtigen, dass die Entwicklung industrieller Standards auch bei größtem Einsatz der Industrie einen hohen zeitlichen Aufwand erfordert. Dies betrifft insbesondere Unternehmen, deren Standardisierungsmaßahmen auf internationaler Ebene abgestimmt werden müssen. Die Umsetzungszeit ist daher zu verlängern. Die Tatsache, dass der Begriff „Stand der Technik“ auch weiterhin gemeinsam durch BSI, KRITIS-Unternehmen und ihre Branchenverbände definiert werden soll, ist positiv. Jedoch bleibt weiterhin kritisch, dass das BSI abschließend über die Geeignetheit branchenspezifischer Standards als „Stand der Technik“ entscheiden kann (§ 8a Abs. 2 BSI-Gesetz). Um Doppelanforderungen und unnötige Bürokratie zu verhindern, schlägt der CSRD vor, die Geeignetheit international anerkannter Standards gesetzlich zu vermuten. Darüber hinaus sollte eine vom Bund unabhängige Schiedsstelle eingerichtet werden, damit Unstimmigkeiten schnell behoben werden können. Schließlich muss sichergestellt werden, dass die Entwicklung und Verifizierung von Standards nicht aufgrund personeller Fehlplanungen durch das BSI gehemmt wird.

2. Kein Konzept für die IT-Sicherheit staatlicher Einrichtungen – In der Kommentierung zum letzten Gesetzesentwurf wurde außerordentlich negativ bewertet, dass das BSI Gesetz keine Regelungen in Bezug auf IT-Systeme des Staates enthält. Diese bilden jedoch wesentliche Faktoren gesellschaftlichen und wirtschaftlichen Zusammenlebens. Diese Kritik wurde nun zum Teil berücksichtigt. Der neue Gesetzesentwurf sieht vor, dass die Sicherheit der IT der Bundesverwaltung ausgebaut werden soll. Umgesetzt wird dies durch die Wiedereinführung des § 8a BSI Gesetz. Im Detail wird jedoch deutlich, dass

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 19.11.2014

das BMI von den Unternehmen mehr fordert, als der Bund bereit ist zu leisten. KRITIS Unternehmen sollen z.B. IT-Mindeststandards einhalten, diese alle zwei Jahre nachweisen und Störungen an das BSI melden. Bundesbehörden hingegen sollen lediglich die vom BSI festgelegten Standards einhalten. Eine Nachweispflicht oder Meldepflicht besteht nicht. Das BSI ist nicht einmal verpflichtet, die Einhaltung zu überprüfen („kann"). Der CSRD fordert, dass der Bund die Bedeutung seiner IT-Infrastruktur angemessen bewertet und konsequenterweise dieselben Sicherheitsanforderungen stellt, wie an private Unternehmen. Nur so kann von einem konsistenten IT-Sicherheitskonzept gesprochen werden. Erforderlich ist weiterhin, dass das BSI mit den nötigen Stellen ausgestattet wird, um diese Aufgaben auch umsetzen zu können. Was die IT-Sicherheitsstruktur der Länder betrifft, die mangels Gesetzgebungskompetenz des Bundes nie Regelungsgegenstand der Entwürfe war, sollten die Länder schnellstmöglich in Absprache mit dem Bund, eine IT-Sicherheitsstrategie erschaffen.

3. Zusammenarbeit zwischen KRITIS und BSI – Der endgültige Entwurf sieht eine „unverzügliche Meldung" des BSI gegenüber den Betreibern kritischer Infrastrukturen vor (§ 8b Abs. 2 BSI-Gesetz). Leistungspflichten und Leistungsfähigkeit des BSI sollten noch weiter ausgebaut und benannt werden. Es genügt nicht, wenn Betreiber kritischer Infrastrukturen über Störungen informiert werden bzw. das BSI über bekannte Abwehrmöglichkeiten informiert. Es sollte vielmehr verpflichtet werden, bei Abwehr von Angriffen Beistand zu leisten. In der Praxis könnte dies durch eine „schnelle Eingreiftruppe" umgesetzt werden, die im Falle erheblicher Angriffe, den betroffenen Unternehmen unverzüglich Hilfe leistet, um die Sicherheit der KRITIS zu gewährleisten. Schließlich ist eine Veränderung des Berichtswesens und die Wiedereinführung eines Quartalsberichts erforderlich.

4. Meldepflicht bei Sicherheitsvorfällen – Die geplante Meldepflicht soll nach dem neuen Entwurf eintreten, wenn eine „erhebliche Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit" eintritt. Damit ändert das BMI erneut den Wortlaut des geplanten Gesetzes (§ 8b Abs. 4 BSI-Gesetz). Erheblich sollen Störungen sein, wenn durch sie die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist. Nach der Begründung (S. 53) sei dies gegeben, wenn die Störung nicht automatisch behoben werden kann bzw. wenn es sich um einen neuartigen oder einzigartigen IT-Vorfall handelt. Tagtäglich vorkommende Ereignisse (z.B. Spam, allgemeine Viren, etc.) sollen nicht erheblich sein.

5. Berücksichtigung Europäischer Vorgaben – Eine umfassende Strategie für Cyber-Sicherheit setzt voraus, dass der gesamte Bereich der IT-Infrastruktur vor Beeinträchtigungen geschützt wird. Vor diesem Hintergrund ist es inkonsequent, dass KRITIS Unternehmen besonders hohe Sicherheitsstandards erfüllen müssen, während an Hard- und Softwarehersteller keine speziellen Anforderungen gestellt werden. Insbesondere mit der *„Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“* (2013/0027(COD)), hätte die Europäische Union einen Beitrag zur Cyber-Sicherheit leisten können. Jedoch wurde im Ergebnis, auch aufgrund deutscher Bemühungen, der Abänderungsvorschlag Nr. 25 angenommen. Danach sollen Hard- und Softwarehersteller aus dem Anwendungsbereich der Richtlinie rausgenommen werden. Sie trifft folglich keine Verpflichtung zur Gewährleistung der Sicherheit und keine Meldepflicht, obwohl sie einen wesentlichen Faktor für die Cyber-Sicherheit in Europa bilden. Der CSRD sieht in dieser Regelung einen wesentlichen Widerspruch zu der geplanten umfassenden Strategie für Cyber-Sicherheit. Erforderlich sind vielmehr neben bereits bestehenden Regelungen zur Produkthaftung, detaillierte Regelungen zum Umgang mit Sicherheitslücken in Hard- und Software. Eine proaktive Strategie muss darauf bestehen, dass die Hersteller von Hard- und Software zum einen verpflichtet werden, Sicherheitsprobleme zu melden und zum anderen diese innerhalb vorgegebener Zeiträume beheben müssen.

6. Zum Erfüllungsaufwand – Der CSRD hat in seiner letzten Stellungnahme kritisiert, dass der Erfüllungsaufwand nicht konkretisiert wurde. Das BMI, hat auf diese Kritik reagiert und nimmt nun den Erfüllungsaufwand an, den es bereits in seinem Entwurf vom 18. August 2014 angenommen hat. Vom Gesamthaushalt des BMI (5,9 Milliarden Euro) werden lediglich 80 Millionen Euro für die Ausstattung seiner zentralen Einrichtung zum Kampf gegen Cyber-Kriminalität also dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zugewiesen. Nach dem Entwurf sollen diese Mittel um 14 Millionen Euro erhöht werden. Damit belaufen sich die Mehrausgaben für den Bereich der Cyber-Sicherheit auf weniger als 0,5 % vom Gesamthaushalt des BSI. Die veranschlagten Mehrausgaben sind willkürlich und beruhen auf Fehlkalkulationen. Dies wird an den geplanten Personalausgaben deutlich. Der Entwurf sieht für das BSI einen Personalaufwand von 67.000 Euro pro Mitarbeiter/Jahr vor. Das durchschnittliche Bruttogehalt einer IT-Fachkraft mit Berufserfahrung liegt jedoch bereits bei

durchschnittlich 75.000 € pro Jahr. Damit wird das BSI nicht in der Lage sein, qualifizierte IT-Fachkräfte zu werben. Der Cyber-Sicherheitsrat fordert die Bundesregierung daher mit Nachdruck dazu auf, die bisherige Strategie zu überarbeiten, um die gesetzten Ziele auch tatsächlich umsetzen zu können. Hierzu gehört zum einen die Aufstockung des BSI mit personellen und sachlichen Mitteln und zum anderen der Abbau von Doppelzuständigkeiten und Bürokratie, die bereits in der Vergangenheit zu einem Scheitern nationaler Einrichtungen, wie dem „Cyber-Abwehrzentrum“ geführt haben.[1] Falls keine zusätzlichen Mittel zur Umsetzung des Gesetzes zur Verfügung gestellt werden, wird sich die bisherige Leistungserbringung des BSI weiter verschlechtern. Das Fehlen konkreter Leistungskennzahlen führt weiterhin dazu, dass der Erfolg bzw. Erfüllungsgrad der Maßnahmen nicht bewertbar ist. Bei einer Umsetzung des derzeitigen Gesetzesentwurfes ist daher vor allem mit der Schaffung eines „Bürokratiemonsters“ zu rechnen, nicht aber mit konkreten Maßnahmen zur Erhöhung der Sicherheit.

7. Weitere Vorschläge zur Erhöhung der IT-Sicherheit – Erklärtes Ziel des Gesetzgebers ist eine signifikante Verbesserung der IT-Sicherheitsinfrastruktur. Daher ist auch positiv zu bewerten, dass die Zuständigkeit des BKA ausgeweitet werden soll. Nach dem endgültigen Entwurf soll das BKA die polizeilichen Aufgaben der Strafverfolgung wahrnehmen soweit es sich um eine Delikt aus § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten), § 202c StGB (Vorbereiten von Ausspähen und Abfangen von Daten), § 263a StGB (Computerbetrug) und § 303a StGB (Computersabotage) handelt und der Angriff gegen Bundeseinrichtungen gerichtet ist. Hierdurch werden unklare Zuständigkeiten vermieden. Jedoch ist zu beachten, dass die vorgeschlagenen Maßnahmen nur gegen äußere Angriffe gerichtet sind. Umso wichtiger ist eine Diskussion über Maßnahmen, mit denen Betreiber kritischer Infrastrukturen auch vor internen Angriffen geschützt werden können. Im Bereich der Luftsicherheit hat der Gesetzgeber bereits Regelungen geschaffen, mit denen Personen, die Zugang zu besonders sensiblen Sicherheitsbereichen haben, auf ihre Zuverlässigkeit hin überprüft werden können. Derartige Zuverlässigkeitsüberprüfungen könnten ein erster Schritt sein, um die Gefahr interner Angriffe im Cyber-Sicherheitsbereich zu minimieren und gleichzeitig den Datenschutz einzuhalten.

[1] http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433

Verfassungsrechtliche Stellungnahme der Knauthe Rechtsanwälte Partnerschaft mbB im Auftrag des Cyber-Sicherheitsrat Deutschland e.V.

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

Executive Summary

1. Der Staat darf die Vorsorge für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen grundsätzlich auf die Betreiber verlagern. Grenzen einer solchen Übertragung von Staatsaufgaben sind aber dort gesetzt, wo dem Staat von Verfassung wegen ausnahmsweise die Erfüllungsverantwortung für die betreffende Aufgabe obliegt. Dies ist nach Art. 87a Abs. 1 S. 1 GG insbesondere für den Bereich der militärischen Landesverteidigung der Fall. Die den Betreibern Kritischer Infrastrukturen auferlegte Pflicht, organisatorische Vorkehrungen gegen Cyber-Zwischenfälle zu treffen, kann dazu führen, dass das betreffende Personal im Fall eines kriegerischen Cyberangriffs unmittelbar an Feindseligkeiten im Sinne des Kriegsvölkerrechts teilnimmt. Solche Tätigkeiten sind aber sowohl völkerrechtlich als auch verfassungsrechtlich den Angehörigen der Streitkräfte vorbehalten. Um die Verfassungsmäßigkeit von § 8a Abs. 1 BSIG-E bzw. § 11 Abs. 1b EnWG-E sicherzustellen, ist daher eine klarstellende Einschränkung des Gesetzeswortlautes erforderlich.

2. Mangels Gesetzgebungskompetenz des Bundes ist es verfassungsrechtlich nicht zu beanstanden, dass das IT-Sicherheitsgesetz (IT-SiG) die Behörden der Länder nicht in die Pflicht nimmt. Auf Grund des Gebots folgerichtiger Gesetzgebung ist es aber verfassungsrechtlich bedenklich, dass Bundesbehörden nicht von der gesetzlichen Definition Kritischer Infrastrukturen erfasst werden und auch im Übrigen keinen vergleichbaren Pflichten zum Schutz ihrer Informationstechnik unterliegen. Nach dem Gebot der Folgerichtigkeit muss sich der Gesetzgeber fragen, ob die betreffende

gesetzliche Regelung in einem inneren Widerspruch zu der Gesamtkonzeption des maßgeblichen Regelungssystems steht. Nach der gebotenen systematisch-teleologische Interpretation ist die Gesamtkonzeption des IT-Sicherheitsgesetzes vor allem darin zu sehen, den Schutz der infrastrukturellen Basis für das Funktionieren des Gemeinwesens zu gewährleisten. Diesem Ziel widerspricht es, wenn Bundesbehörden keinen vergleichbaren IT-Schutz gewährleisten müssen. Bundesbehörden sind zu einem großen Teil ebenso kritisch für das Funktionieren des Gemeinwesens, wie private Infrastrukturen und daher auch mit vergleichbaren Vorgaben hinsichtlich der Sicherheit ihrer Informationstechnik zu belegen.

3. Die fehlende Einbeziehung der Hersteller informationstechnischer Produkte und Systeme in die Sicherheitsvorsorge für die Informationstechnik in Kritischen Infrastrukturen dürfte gegen Art. 3 Abs. 1 GG verstoßen. Innerhalb der Vergleichsgruppe derjenigen Akteure, die mit Informationstechnik in Kritischen Infrastrukturen wesentlich in Berührung kommen, werden die Betreiber gegenüber den Herstellern dadurch benachteiligt, dass allein sie Sicherungspflichten treffen. Für diese Ungleichbehandlung besteht kein rechtfertigender Grund. Insbesondere sind die Betreiber nicht besser zur Gefahrenbeherrschung in der Lage, als die Hersteller der entsprechenden informationstechnischen Produkte und Systeme. Fehler in informationstechnischen Produkten und Systemen sind in der Regel die unmittelbare Ursache für Gefährdungen der Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Von daher verfügen auch die entsprechenden Hersteller über die besten Gefahrenabwendungsmöglichkeiten und Kenntnisse über mögliche Gefahren für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Ihre Tätigkeit ist somit sachnäher als die der Betreiber und sie ist daher ebenfalls mit Pflichten im Hinblick auf die Sicherheit in der Informationstechnik Kritischer Infrastrukturen zu belegen, um einen Verstoß gegen Art. 3 Abs. 1 GG zu vermeiden.

4. Soweit die Vorgaben des IT-Sicherheitsgesetzes dazu führen, dass Betreiber Kritischer Infrastrukturen strengeren Vorgaben unterliegen, als sie bereits auf Grund internationaler Anforderungen unterliegen, so liegt darin im Falle von unzumutbaren Mehrkosten bei fehlendem finanziellen Ausgleich ein Verfassungsverstoß. Das Interesse an einem wirksamen Schutz der Informationstechnik in Kritischen Infrastrukturen ist wegen der weitreichenden gesellschaftlichen Folgen eines Ausfalls der betreffenden Dienstleistungen kein Gruppen-, sondern ein Allgemeininteresse.

Die Lasten solcher öffentlichen Angelegenheiten haben grundsätzlich die Allgemeinheit zu treffen und sind demnach im Wesentlichen durch die Gemeinlast Steuer zu finanzieren.

5. Es ist nicht verfassungsrechtlich geboten, dass alle Einrichtungen, Anlagen oder Teile, die Kritische Infrastrukturen sein sollen, bereits im Gesetz aufgezählt werden. Verfassungsrechtlich geboten ist aber eine nähere parlamentsgesetzliche Bestimmung des definitorischen Rahmens, in dem sich die Bestimmung durch den Verordnungsgeber vollziehen soll. Die vom Bundesverfassungsgericht entwickelte Wesentlichkeitstheorie und Art. 80 Abs. 1 S. 2 GG besagen, dass im Bereich der Normsetzung durch die Exekutive "wesentliche Entscheidungen" durch das Parlament selbst getroffen werden müssen. Je wesentlicher die übertragene Materie für den Gesetzgeber beziehungsweise je schwerwiegender/grundrechtsrelevanter die Auswirkungen für die Betroffenen sind, desto größer muss die Bestimmtheit der entsprechenden Norm sein. Wegen der erheblichen Auswirkungen auf Grundrechte der betroffenen Unternehmen, genügt es nicht, in § 2 Abs. 10 BSIG-E nur eine sektorenbezogene Bestimmung vorzunehmen. Vielmehr dürfte auch die Nennung konkreter Branchen und der in den jeweiligen Branchen als kritisch anzusehenden Dienstleistungen erforderlich und, etwa mittels Anlagen zum Gesetz, auch möglich sein.

6. Die Zuständigkeitserweiterung der Bundesnetzagentur durch das IT-Sicherheitsgesetz ist als solche verfassungsrechtlich unbedenklich. Bedenklich ist jedoch, dass die Betreiber von Energieversorgungsnetzen und die Betreiber von Energieanlagen für das Vorliegen des gesetzlich gebotenen "angemessenen Schutzes" den Sicherheitskatalog der Bundesnetzagentur zwingend einhalten müssen, während andere Betreiber Kritischer Infrastrukturen nicht an einen ähnlichen Katalog gebunden sind, sondern verschiedene Möglichkeiten haben, für einen angemessen Schutz ihrer Informationstechnik zu sorgen und dies nachzuweisen. Diese Ungleichbehandlung zwischen den verschiedenen Betreibern dürfte einen Verstoß gegen Art. 3 Abs. 1 GG darstellen. Eine gegenüber anderen Betreibern Kritischer Infrastrukturen womöglich herausgehobene Stellung der Betreiber von Energieanlagen bzw. Energieversorgungsnetzen vermag den Ausschluss der den Betreibern anderer Kritischer Infrastrukturen nach § 8a Abs. 2, 3 S. 2 BSIG-E offerierten Möglichkeiten nicht verfassungsrechtlich zu rechtfertigen.

7. Die nach dem IT-Sicherheitsgesetz vorgesehene Sicherungspflicht gegen Störungen der Informationstechnik in Kritischen Infrastrukturen und die Meldepflicht für erhebliche Störungen verstößt gegen verschiedene Grundrechte der Betreiber. Vor allem liegt ein unverhältnismäßiger Eingriff in die Berufsfreiheit der betroffenen Betreiber vor. Dies gilt allerdings nur für den vermögensbelastenden - weil kompensationslosen -, nicht aber für den verhaltensregelnden Eingriff in Gestalt der Pflichten als solchen. Als vermögensbelastender Eingriff sind die Sicherungs- und die Meldepflicht deshalb unverhältnismäßig, weil sie zu erheblichen Mehrkosten in Form von Personal- und Sachkosten führen, die auch angesichts der hohen Bedeutung der verfolgten Belange unzumutbar erscheinen und die Betreiber zudem gegenüber anderen privaten Dienstleistern für das öffentliche Wohl, die für ihre Tätigkeit eine Entschädigung erhalten, in verfassungsrechtlich nicht gerechtfertigter Weise benachteiligen. Hinsichtlich der Meldepflicht kommt vor allem ein Verstoß gegen das Recht auf informationelle Selbstbestimmung hinzu, der darauf zurückzuführen ist, dass der Gesetzesentwurf weder die Art der zu meldenden Vorfälle hinreichend bestimmt, noch den Zweck der Datenerhebung eindeutig genug kennzeichnet und somit nicht dem bei Eingriffen in das Recht auf informationelle Selbstbestimmung besonders bedeutsamen Gebot der Normenklarheit genügt.