Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 4.11.2014

12.11.14
Seite 1

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. Am 4. November 2014 hat das Bundesministerium den dritten Referentenentwurf veröffentlicht, obwohl dieser noch nicht innerhalb der Bundesregierung abgestimmt ist. Der CSRD möchte dennoch die Gelegenheit wahrnehmen, seine Position zu diesem Entwurf darzulegen.

Zusammenfassung

- Der Aufwand für die Betreiber Kritischer Infrastrukturen, d.h. Energie, Finanzen, Logistik, Telekommunikation, Gesundheit, ab 10 Mitarbeitern und einem Jahresumsatz von mehr als 2 Mio. Euro, ist realistischer Weise nicht umsetzbar, zu kostenintensiv und bürokratisch.
- Der Bund selbst und seine Verwaltung verstehen sich nicht als Kritische Infrastrukturen und halten das Gesetz für nicht praktikabel, weshalb sie sich von dessen Umsetzung ausnehmen. Die Bundesländer, die auch wesentliche KRITIS, wie beispielsweise die Polizeien, betreiben, bleiben ebenfalls unberücksichtigt.
- Die Einbindung der verursachenden Industrie (Soft- und Hardwarehersteller) wird vernachlässigt.
- Der Bund hat keine konsistente Cyber-Sicherheitsstrategie, die die verschiedenen Belange von Wirtschaft, Wissenschaft und Strafverfolgung berücksichtigt. Durch die Einführung des Gesetzes wird die Bürokratie ausgebaut ohne die Leistungsfähigkeit des Staates zu erhöhen. Am Ende wird das Gesetz in seiner aktuellen Fassung sogar zu deutlich weniger Sicherheit führen.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 4.11.2014

1. Branchenspezifische Mindestanforderungen – Der CSRD begrüßt die Einführung branchenspezifischer Mindeststandards an die IT-Sicherheit (sog. „Stand der Technik"). Kritisch ist aber noch immer 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.
Darüber hinaus 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. Insbesondere die Tatsache, dass keine Angaben dazu gemacht werden, was auf staatlicher Seite mit den gesammelten Meldungen getan wird, erhöht hierbei nur die Unsicherheit auf Seiten der KRITIS. So ist beispielsweise auch nicht definiert, wie damit umzugehen ist, wenn Rechenzentren außerhalb Deutschlands betrieben werden. Hinzu kommen unklare Verantwortlichkeiten im Bereich der Strafverfolgung und Unterstützung im Falle von IT-Sicherheitsvorfällen.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 4.11.2014

2. Kein gemeinsames Konzept für Bund, Länder und Kommunen – Besonders negativ ist zu bewerten, dass der Staat als größter Betreiber Kritischer Infrastrukturen nicht unter das Gesetz fallen soll. Damit verlangt der Staat von den Unternehmen mehr, als er selbst bereit ist zu leisten. Für den Bund war eine entsprechende Regelung im zweiten Entwurf vorgesehen (§ 8 Abs. 1 BSI-Gesetz). Die ersatzlose Streichung dieser Regelung entzieht dem dritten Entwurf die Glaubwürdigkeit und unterstreicht nur, dass auf Seiten des Bundes eine tatsächliche Umsetzung als nicht praktikabel erachtet wird. Eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland wird so zumindest nicht erreicht werden können. Dies gilt erst Recht im Hinblick auf die IT-Sicherheitsstruktur der Länder, die mangels Gesetzgebungskompetenz des Bundes nie Regelungsgegenstand der Entwürfe war. Erforderlich ist daher nicht nur eine gesetzliche Regelung für den Bund, sondern die Schaffung einer länderübergreifenden IT-Sicherheitsstrategie.

3. Zusammenarbeit zwischen KRITIS und BSI – Auch der neue Entwurf sieht vor, dass die Zusammenarbeit zwischen Staat und Betreibern Kritischer Infrastrukturen verbessert werden soll (S. 2). Nachdem der CSRD in seinen vorherigen Stellungnahmen deutlich gemacht hat, dass die gesetzliche Regelung diese Zielvorgabe nicht umsetzt, wurde nun nachgebessert. Der aktuelle Entwurf sieht wieder eine „unverzügliche Meldung“ des BSI gegenüber den Betreibern kritischer Infrastrukturen vor. Leistungspflichten und Leistungsfähigkeit des BSI sollten jedoch noch weiter ausgebaut werden.
So setzt eine effektive Abwehr von Cyberangriffen voraus, dass das BSI anhand der gewonnenen Erkenntnisse Warnungen und Hilfestellungen zur Verfügung stellt. Ein erster Schritt wäre die Veränderung des Berichtswesens und die Wiedereinführung eines Quartalsberichts. Überdies sollte das BSI über eine „schnelle Eingreiftruppe“ verfügen. Es sollte verpflichtet werden, im Falle erheblicher Angriffe, den betroffenen Unternehmen unverzüglich Hilfe zu leisten, um die Sicherheit der KRITIS zu gewährleisten. Darüber hinaus sollten die gesammelten Erkenntnisse an die Strafverfolgungsbehörden, zur Aufklärung und Verhinderung zukünftiger Straftaten, weitergeleitet werden.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 4.11.2014

4. Zum Erfüllungsaufwand – Der CSRD hat in seiner letzten Stellungnahme deutlich gemacht, dass der vorgeschlagene Erfüllungsaufwand in keinem Verhältnis zu den Schäden durch Cybercrime und dem Budget des BMI steht. Der Umstand, dass der Erfüllungsaufwand im neuen Entwurf nicht ausgewiesen wurde bzw. noch als „Gegenstand von Erörterungen zwischen den Ressorts“ (S. 4) gilt, verdeutlicht, dass die Politik kein klares Konzept verfolgt. Andernfalls ist nicht erklärbar, warum im dritten Referentenentwurf auf diese Angaben verzichtet wurde. Mehr noch: Solang keine konkreten Ressourcen beim BSI genannt werden, bleibt unklar, ob und wieviel der Staat investieren will. 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.

5. Meldepflicht bei Sicherheitsvorfällen – Die geplante Meldepflicht soll nach dem neuen Entwurf eintreten, wenn eine „bedeutende Störung“ der IT-Systeme vorliegt (§ 8b Abs. 4 BSI-Gesetz) und ersetzt damit weitestgehend das Merkmal der „Beeinträchtigung“. Durch den Verweis auf die höchstrichterliche Rechtsprechung zu § 100 Abs. 1 TKG (Begründung, S. 40) soll so eine noch genauere Bestimmung der Meldepflicht möglich werden. Leider ist auch die aktuelle Definition nicht geeignet, um den Eintritt der Meldepflicht ausreichend zu konkretisieren. Fraglich ist insbesondere, wann die Funktionsfähigkeit des Betreibers oder der KRITIS bedroht ist. Ist dies bereits der Fall, wenn ein unbefugter Datenzugriff erfolgt oder muss die Störung auf den konkreten Betriebsablauf einwirken? In der Praxis werden diese Fragen täglich auftreten. Positiv ist daher nur, dass der Entwurf weiterhin an der anonymen Meldepflicht festhält und nur in besonders schwerwiegenden Fällen eine namentliche Meldepflicht vorsieht.

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 4.11.2014

6. 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.

7. Weitere Vorschläge zur Erhöhung der IT-Sicherheit – Erklärtes Ziel des Gesetzgebers ist eine signifikante Verbesserung der IT-Sicherheitsinfrastruktur. 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.