/ Bundestag beschließt IT-Sicherheitsgesetz – ein Schritt Richtung sichere IT?

18.06.2015

IT & Outsourcing | Datenschutz

Am letzten Freitag, den 12. Juni 2015 hat der Deutsche Bundestag das schon seit längerem in der Diskussion befindliche IT Sicherheitsgesetz beschlossen. Das IT-Sicherheitsgesetz stellt ein wichtiges Schlaglicht der digitalen Agenda der Bundesregierung dar. Ziel des Gesetzes ist es den praktisch immer wichtiger werdenden, zugleich aber gesetzgeberisch bislang kaum berührten, Bereich der IT-Sicherheit regulatorisch zu erfassen.

Dieses Ziel des Gesetzesvorhabens ist im Grundsatz zu begrüßen, denn in der digitalisierten Welt sind zwei Entwicklungen zu beobachten, die zu einer signifikanten Erhöhung der Bedrohungslage im Cyberraum führen und dabei Regierung, Wirtschaft und Bevölkerung vor erhebliche Herausforderungen stellen:

1. Die Abläufe und Prozesse in der Regierungsarbeit, der Wirtschaft (Stichwort: **Industrie 4.0**) und dem Alltag werden zunehmend abhängiger von – immer stärker vernetzten –informationstechnischen Systemen; und damit anfälliger für Cyberangriffe.

2. Gleichzeitig erfolgen Cyberangriffe zunehmend zielgerichteter und mit technologisch ausgereifteren Mitteln.

Wie groß diese Gefahren tatsächlich sind, zeigte erst jüngst der – erfolgreiche – Hackerangriff auf die IT-Systeme des Bundestags selbst. Ob das IT-Sicherheitsgesetz in seiner derzeitigen Fassung ausreichend und geeignet ist, um diesen Gefahren zu begegnen und die Sicherheit informationstechnischer Systeme in Deutschland signifikant zu verbessern, – wie es der Gesetzesentwurf selbst als Ziel des Gesetzes ausgibt – darf jedoch in Zweifel gezogen werden.

1. Struktur und wesentliche Inhalte des Gesetzes

Anders als der Titel des Gesetzes es vermuten lässt, sieht das IT-Sicherheitsgesetz nicht die Schaffung eines eigenen Gesetzes zur IT-Sicherheit vor. Vielmehr führt es zu einer Änderung verschiedener Einzelgesetze, vor allem des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), des Telemediengesetzes, des Telekommunikationsgesetzes und des Energiewirtschaftsgesetzes.

Im Wesentlichen haben die Gesetzesänderungen folgende Inhalte:

BSI Gesetz

- An mehreren Ecken im Entwurf wird dem Ziel, das **Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Aufsichtsbehörde** für IT-Sicherheit zu etablieren, Rechnung getragen.

- Die neuen Anforderungen im BSI Gesetz **betreffen alle *„Betreiber kritischer Infrastrukturen“***. Welche dies sind, soll gem. des (neu vorgesehenen) § 2 Abs. 10 des BSI Gesetzes das Bundesministerium des Innern in einer Rechtsverordnung bestimmen.

- Der neue § 8b Abs. 4 BSI Gesetz sieht eine **Meldepflicht** der Unternehmen bei erheblichen Störungen ihrer IT-Systeme vor, die die *„Kritischen Infrastrukturen“* beeinträchtigen könnten. Die Meldungen sollen direkt an das BSI erfolgen, wobei eine **pseudonyme Meldung grundsätzlich ausreicht**. Eine **namentliche Nennung** soll allerdings erforderlich sein, wenn die ***„Kritische Infrastruktur“* ausfällt oder beeinträchtigt** wird.

- Gem. dem neuen § 8a Abs. 1 BSI Gesetz sind die betroffenen Unternehmen verpflichtet innerhalb eines Zeitraums von zwei Jahren ab Inkrafttreten der Rechtsverordnung die die Kritischen Infrastrukturen bestimmt ***„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“*** unter Berücksichtigung des aktuellen Stands der Technik zu treffen.

- Branchenverbände (und *„Betreiber Kritischer Infrastrukturen“)* haben gem. des neuen § 8a Abs. 2 BSI Gesetz die Möglichkeit dem BSI **Sicherheitsstandards für ihre jeweilige Branche vorzuschlagen**.

- § 8a Abs. 3 BSI Gesetz sieht in diesem Zusammenhang weiter eine Verpflichtung der Unternehmen vor, dem BSI mindestens alle zwei Jahre und darüber hinaus im Fall von festgestellten Sicherheitsmängeln eine **Aufstellung aller Sicherheitsaudits, Prüfungen und Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel zu übermitteln**.

- Bemerkenswerterweise erst in der letzten Revision haben **Bußgeldvorschriften** Einzug in das Gesetz gefunden. § 14 BSI Gesetz sieht nunmehr Bußgelder zwischen EUR 50.000,00 und EUR 100.000,00 für bestimmte Verstöße gegen das BSI Gesetz vor, die insbesondere **im Falle unzureichender IT-Sicherheitsmaßnahmen** greifen, bzw. dann wenn **trotz tatsächlicher Beeinträchtigung einer *„Kritischen Infrastruktur“* keine Meldung** erfolgt.

- Möglicherweise vor dem Hintergrund des erfolgreichen Angriffs auf die IT-Systeme des Bundestags selbst wurde in der letzten Revision noch eine **Verpflichtung des BSI** aufgenommen, **Mindeststandards für die Sicherheit der IT-Systeme des Bundes zu erarbeiten**. Zuvor bestand lediglich eine Ermächtigung des BSI, solche Standards zu erarbeiten, jedoch keine Verpflichtung.

Telemediengesetz

- Das Telemediengesetz erhält einen neuen § 13 Abs. 7, der **Anbietern von Telemedien** eine Pflicht zur Einhaltung **bestimmter technisch-organisatorischer Maßnahmen** auferlegt.

Telekommunikationsgesetz

- **Ähnliche Pflichten wie für die Betreiber *„Kritischer Infrastrukturen“*** sieht der neu gefasste § 109 des Telekommunikationsgesetzes auch **für alle Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste** vor.

- In dem neuen § 100 Abs. 1 des Telekommunikationsgesetzes erhalten **Telekommunikationsanbieter weitgehende Befugnisse Verkehrsdaten der Nutzer zu verarbeiten** (insbesondere diese zu speichern und zu erheben), soweit dies dazu dient Störungen oder Fehler der Telekommunikationsanlagen zu erkennen oder zu beseitigen.

2. IT-Sicherheitsgesetz = sichere IT?

Ob das IT-Sicherheitsgesetz in seiner derzeitigen Form geeignet ist einen erheblichen Beitrag zur Verbesserung der IT-Sicherheit zu leisten wird insbesondere **von IT-Sicherheitsexperten bezweifelt**. Auch **datenschutzrechtlich** stößt das IT-Sicherheitsgesetz auf **Bedenken**, da es durch die Änderung in § 100 Abs. 1 TKG eine weitgehende Erlaubnis für Telekommunikationsanbieter vorsieht Daten über das Verhalten der Nutzer zu speichern. Es steht zu befürchten, dass auf diesem Wege eine **Vorratsdatenspeicherung „durch die Hintertür“** eingeführt wird.

Darüber hinaus enthält das IT-Sicherheitsgesetz viele **Formulierungen und Verpflichtungen deren praktische Auswirkungen ungewiss sind** und die in ihrer Unbestimmtheit d**em BSI letztlich einen sehr weiten Interpretationsspielraum zugestehen**.

- Augenfällig ist insbesondere, dass **keinerlei konkrete Vorgaben für die einzuhaltenden IT-Sicherheitsmaßnahmen** gemacht werden – stattdessen ist lediglich die Rede von *„angemessenen“* Maßnahmen. Zwar bedarf es vor dem Hintergrund der rasanten technischen Entwicklung durchaus einer flexiblen Formulierung – wünschenswert wäre es jedoch gewesen zumindest die Kriterien weiter zu beschreiben, insbesondere unter Berücksichtigung von Risikoanalysen und konkretisierbaren Gefahrenlagen. Es bleibt zu hoffen, dass hier die Branchenverbände von der Möglichkeit branchenweite Sicherheitsstandards vorzuschlagen, auch tatsächlich Gebrauch zu machen, um so zumindest ein gewisses Maß an Rechtssicherheit zu schaffen.

- Auch im Übrigen enthält das IT-Sicherheitsgesetz **zahlreiche weitere dergestalt unbestimmte Formulierungen**. Insgesamt lässt sich zum jetzigen Zeitpunkt nur konstatieren, dass das IT-Sicherheitsgesetz auch aus juristischer Sicht in vielen Bereichen eher Unklarheit denn Rechtssicherheit bringt.

- Hier bleibt derzeit nur zu hoffen, dass sich eine **einheitliche und handhabbare Aufsichtspraxis des BSI** herausbildet, die das BSI dann auch offen kommuniziert – vergleichbar der MaRisk im bankaufsichtsrechtlichen Bereich oder der „Orientierungshilfe Cloud Computing“ im datenschutzrechtlichen Bereich.

Wenig glücklich erscheint darüber hinaus, dass das **IT-Sicherheitsgesetz unabhängig von** der sich am Horizont bereits abzeichnenden **EU Richtlinie zur Netz- und Informationssicherheit (NIS)** beschlossen wurde. Soweit die NIS mit von dem IT-Sicherheitsgesetz abweichenden Inhalten beschlossen wird, dürfte schon kurz nach dessen Inkrafttreten eine Revision des IT-Sicherheitsgesetzes notwendig werden.

Haben Sie Fragen? Kontaktieren Sie gerne Stefan Wilmer

Practice Group: IT, Outsourcing & Datenschutz

Weitere Artikel: EU-Datenschutz-Grundverordnung: EU-Minister erzielen Einigung auf europaweite Standards ; Data Breaches: 5 Praxistipps

Contact Person

Prof. Dr. Peter Bräutigam
Mitglied der Practice Group Digital Business
Mitglied der Practice Group Versicherung & Rückversicherung
Rechtsanwalt, Fachanwalt für Informationstechnologierecht

T +49 89 28628145