Das neue IT-Sicherheitsgesetz ("Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme")

Dienstag, 25. August 2015

Das neue IT-Sicherheitsgesetz ("Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme")

(1) Einleitung

Angesichts zunehmender Cyberangriffe hat der Bundestag am 12.06.15 das „IT-Sicherheitsgesetz“ verabschiedet, das nun am 24.07.15 in Kraft getreten ist. Grundsätzlich handelt es sich um ein „Artikelgesetz“, d.h. es ist kein neues, eigenständiges Gesetz, sondern es handelt sich um die Überarbeitung bzw. Ergänzung bestehender Gesetze. Diese Änderungen betrafen:

- BSI-Gesetz
- Telekommunikationsgesetz (TKG)
- Telemediengesetz (TMG)
- Atomgesetz
- Energiewirtschaftsgesetz

Im nachfolgenden wird auf die Änderungen eingegangen, die das BSI-Gesetz, das TKG und das TMG betreffen.

(2) BSI-Gesetz

Das BSI-Gesetz definiert die Rolle, die Position und die Rechte des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Mit den Änderungen wird diese Rolle präzisiert und das BSI in seinen Rechten gestärkt. So kann das BSI z.B. auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme auf Sicherheitsaspekte hin untersuchen und diesbezügliche Erkenntnisse weitergeben und veröffentlichen. In Zukunft fungiert es zudem als zentrale Meldestelle für IT-Sicherheitsvorfälle.

Weiterhin findet sich im BSI-Gesetz vor allem die grundlegende Definition der “kritischen Infrastrukturen“, auf die das IT-Sicherheitsgesetz Anwendung finden soll. Dies sind nun insbesondere:

„Einrichtungen, …, die den Sektoren Energie, Informationstechnik und Telekommunikation; Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören“. Für diese Betreiber hält das BSI-Gesetz nun fest, dass sie spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung (…) angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen müssen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Die Erfüllung der Anforderungen haben Betreiber alle zwei Jahre auf geeignete Weise nachzuweisen (z.B. Sicherheitsaudits, Prüfungen, Zertifizierungen).

Weiterhin sind die Betreiber kritischer Infrastrukturen verpflichtet, innerhalb von sechs Monaten nach Inkrafttreten des Gesetzes eine Kontaktstelle für das Bundesamt für Informationssicherheit (BSI) einzurichten, über die der Betreiber jederzeit erreichbar ist. Über diese Kontaktstelle melden die Betreiber erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit in ihren Systemen.

Ausgenommen von diesen Bestimmungen sind Betreiber kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz oder öffentlich zugängliche TK-Dienste betreiben. Die Informationspflichten dieser Anbieter bei Sicherheitsvorfälle und zu ergreifende IT-Sicherheitsmaßnahmen finden sich im TKG, sowohl in dem bereits bestehenden Teilen des TKGs wie den aktuellen Änderungen.

(3) Telekommunikationsgesetz (TKG)

Im TKG werden bereits bestehende Regelungen über die Behebung und Information von Störungen dahingehend ergänzt, dass IT-Sicherheitsvorfälle als „Störungen“ definiert werden. So durfte laut bisherigen § 100 TKG der Dienstanbieter bereits Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler einzugrenzen und zu beseitigen. Hier werden jetzt auch explizit Störungen eingeschlossen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff führen können.

Auch die bisherige Fassung des § 109 (4) TKG beinhaltete bereits die Pflicht von Betreibern öffentlicher TK-Netze bzw. öffentlich zugängliche TK-Dienste, ein Sicherheitskonzept vorzulegen. Geändert hat sich hier, dass - statt einer pauschalen Aussage, dass die Bundesnetzagentur dieses prüfen kann - die Bundesnetzagentur dieses Konzept alle zwei Jahre prüft.

Die Informationspflichten der Betreiber bezüglich möglicher Störungen an die Bundesnetzagentur werden im Hinblick auf IT-Sicherheitsverletzungen präzisiert. Es erfolgt nun eine Information der Bundesnetzagentur an das BSI über mögliche Sicherheitsverletzungen.

Weiterhin enthielt der nachfolgende § 109a TKG die Pflicht des TK-Anbieters, im Falle von einer schwerwiegenden Verletzung des Schutzes personenbezogener Daten den Betroffenen zu informieren. Nun entstehen diese Informationspflichten auch, wenn Störungen bekannt werden, die vom Datenverarbeitungssystemen des Nutzers ausgehen, wobei der Betreiber den Nutzer darauf aufmerksam machen muss, wie die Störungen erkannt und beseitigt werden können.

(4) Telemediengesetz (TMG)

Im TMG wurde namentlich der folgende Artikel geändert – in Zukunft gilt § 13 (7) in der neuen Formulierung:

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
kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
diese 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.

(Der bisherige Absatz 7 wird Absatz 8)

(5) Fazit

Kaum ein Gesetz wird erlassen, ohne dass sich nicht zahlreiche Juristen und Verbände ihre Kritik hierzu äußern. Der häufig gebrauchte, sicherlich nicht unberechtigte Vorwurf, dass neue Gesetze zur Bürokratisierung beitragen, wurde auch hier geäußert. Juristen beklagen aber auch die unscharfen Formulierungen des Gesetzes. Z.B. werde zu unpräzise formuliert, was wann gemeldet werden muss oder was genau „Stand der Technik“ sei. Auch wird nicht festgehalten, welche „Zertifizierungen“ im BSI-Gesetze als solche auch anerkannt werden.

Kritisiert wird auch, dass der Wirkungskreis auf Betreiber „kritischer Infrastrukturen“ beschränkt sei. Angreifer nutzen typischerweise aber Schwächen bei Unternehmen der unterschiedlichsten Branchen aus, die die Software nutzen und oft keinen Zugriff auf die Systeme selbst haben.

Bei aller Kritik kann dieses Gesetz aber als ein erster Schritt in einem Bereich betrachtet werden, der zum aktuellen Zeitpunkt so gut wie gar nicht geregelt wird, in dem Unternehmen aber immer mehr Schaden erleiden. Welche der Regelungen praxistauglich ist und was noch ergänzt oder geändert werden muss, wird die Zukunft erweisen.

Dieser Artikel gibt nur einen ersten Einblick in die Gesetzesänderungen geben. Die kompletten Gesetzesänderungen werden im Bundesgesetzblatt veröffentlicht.

Quelle: Bundesministerium des Inneren (Gesetzesentwurf [1] und Meldung [2]vom 24.07.15)

Autor: Christine Thieme
Copy: Erledigt

Links
[1] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile
[2] http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2015/07/it-sicherheitsgesetz-tritt-in-kraft.html?nn=3446780