**Anmerkungen zum**
**‚Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme‘**

[Bearbeitungsstand 25.3.13 11.30 Uhr]

1 Der vorliegende Entwurf eines **Artikelgesetzes** modifiziert die folgenden Gesetze:
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
- Bundeskriminalamtgesetz
- Telemediengesetz
- Telekommunikationsgesetz.

2 **Ziel** des Gesetzes ist die Erhöhung des Sicherheitsniveaus deutscher Unternehmen aus dem Bereich Kritischer Infrastrukturen im Internet – u.a. durch Sicherungspflichten, die dem Stand der Technik entsprechen müssen und eine **Meldepflicht:** ‚erhebliche IT-Sicherheitsvorfälle‘ sollen von Betreibern kritischer Infrastrukturen dem Bundesamt für IT-Sicherheit (BSI) gemeldet werden. Anbieter von Internetdiensten unterliegen allerdings bereits heute schon einer Meldepflicht gem. TKG.

Das Ziel einer besseren Abwehr von Internetangriffen soll durch Sicherungspflichten in § 13 TMG und § 109 TKG erreicht werden; kann durch das **Zählen** von ‚Sicherheitsvorfällen allerdings‘ nicht erreicht werden. Die ausschließliche Meldung von Angriffen geht also in die falsche Richtung: **Sicherheit wird nur vorgetäuscht**.

3 **Adressaten** des Gesetzes sind vor allem das BSI und das BKA aber auch die Betreiber kritischer Infrastrukturen, Telekommunikations- und Telemediendiensteanbieter wie Finanzdienste, Verkehr, Energie und Gesundheitswesen), Betreiber zentraler Dienste der Informationsgesellschaft (vor allem App-Stores, eCommerce-Plattformen, Internet-Zahlungen, Cloud-Computing, Suchmaschinen, soziale Netze) und öffentliche Verwaltungen. Die Softwarehersteller werden nicht adressiert. Betreiber, die Software beschaffen, müssen diese nach den Anforderungen des Gesetzes auswählen. Ob ein Betreiber aber die im Betrieb befindliche Software ändern kann und darf oder den Hersteller dazu verpflichten kann, ist abhängig von der jeweiligen vertraglichen Stellung und der Marktmacht der Beteiligten. Dieses Problem wird vom Gesetzentwurf nicht angesprochen oder gar gelöst.

4 Als **Begründung** für das Gesetz werden pauschal genannt:
- IT-Ausfälle – die werden aber im Weiteren gar nicht adressiert und
- stetig zunehmende Angriffe, gestiegene Bedrohungslage

An keiner Stelle werden über diese sehr pauschalen Behauptungen hinaus Zahlen genannt. Die weitaus meisten IT-Ausfälle dürften rein technische Hardware-Ursachen haben und auf funktionale Fehler in der Software zurückgehen. Angriffe werden weit überwiegend erkannt und abgewehrt. Die pauschalen Gesetzes- und Begründungsformulierungen legen den Schluss nahe, dass dem Bundesinnenministerium über die Anzahl und den Schweregrad von Angriffen keinerlei belastbare Untersuchungen vorliegen.

5 Mit der bereits 2012 vom Innenminister Friedrichs für die Bundesrepublik angesprochenen Meldepflicht von Angriffen und in 2013 von der EU-Telekomkommissarin Neelie Kroes für die gesamte EU erneut vorgeschlagenen Richtlinie zur sog. Netz- und Informationssicherheit zur Meldepflicht von Angriffen und ‚Datenpannen‘ an den Staat kann das Internet nicht vor kriminellen und terroristischen Angriffen geschützt werden: Melden allein schützt nicht! Das wird durch die Vorlage eines – mit dem Bundeskabinett nicht abgestimmten - Gesetzentwurfs durch das BMI im März nicht besser.

6 Die unter B. Lösung formulierte Rolle des BSI zur IT-Sicherheit kritischer Infrastrukturen wird insgesamt gestärkt durch die Aufgabe, auf Ersuchen bei der Sicherung der Informationstechnik zu beraten und unterstützen.‘ ist falsch: Im Gesetzestext ist dies eine ‚Kann‘-Regelung; d.h. das BSI **kann** beraten, muss aber nicht und kann (ohne Begründung) die Beratung ablehnen.

7 Unklar bleibt, was mit den folgenden Begriffen gemeint sein könnte , … die für das Rückgrat der Informationsgesellschaft verantwortlichen Anbieter (sollen durch Melden) zu einem ‚**validen und vollständigen Lagebild**‘ der IT-Sicherheit beitragen‘. In jedem Fall müssen aus den aufsummierten Meldungen Maßnahmen abgeleitet werden wie Verpflichtung
- (vor allem?) der Hersteller von Software zur Identifizierung von Sicherheitslücken
- zur Information von Kunden von Software-Anbietern über die ausgenutzten Sicherheitslücken und Mängel
- der Hersteller von Software generell zur Behebung von Sicherheitslücken.

8 § 8a Ziff. 4: Es bleibt allerdings unklar, wie ein ausländischer Hersteller einer Software durch das BSI-Gesetz zur **Beseitigung eines Sicherheitsmangels** verpflichtet werden kann. Der Endanwender dürfte jedenfalls aus Lizenz-rechtlichen und tatsächlichen Gründen grundsätzlich keine Sicherheitslücken beheben können.

9 Telekommunikationsanbieter sollen betroffene Nutzer über Störungen durch Schadprogramme informieren: Damit könnte die - weitgehend abgelehnte - **deep packet inspection** gemeint sein.

10 Zu Art. 4 (Änderung des Telekommunikationsgesetzes) wird zur Nummer 1 (§ 109 Technische Schutzmaßnahmen) im 3. Absatz plötzlich wertend (‚Angriffe auf höchstem technischem Niveau' – tatsächlich sind solche seit 2007 in Deutschland bekannt) ausgeführt, dass zunehmend bislang nicht-erkannte Sicherheitslücken (**Zero-Day-Vulnerabilities**) ausgenutzt werden. Falsch ist die Bemerkung, dass diese nur in der Sicherheitsarchitektur von Hardware und Software auftreten – richtig ist vielmehr, dass sie auch im Quellcode sowie in dem (ausführbaren) Maschinencode auftreten. Dies ist die (einzige) [falsche] Definition des Begriffs ‚Angriff'.

11 Große Unternehmen aus dem Bereich Kritische Infrastrukturen werden 400.000-mal pro Tag angegriffen. Bei ca. 10.000 relevanten Unternehmen (und Behörden!) in der EU ergeben sich bei durchschnittlich nur 1.000 Angriffen pro Tag **10 Mio. Datensätze**, die ja auch täglich abschließend und vollständig europaweit ausgewertet werden müssten: **Sammeln allein macht nicht sicher**.

12 Angriffe auf das Internet und die IT von Unternehmen sind nur dann erfolgreich, wenn Software **Sicherheitslücken** enthält, die von Angriffen ausgenutzt werden können – anderenfalls laufen Angriffe ‚gegen die Wand'. Um Angriffe in den Griff zu bekommen, müssen daher die ausgenutzten Sicherheitslücken identifiziert und dann auch behoben werden: **Das Übel an der Wurzel packen**!

Sicherheitslücken werden allerdings von einigen Software-Herstellern nur zur Kenntnis genommen und nicht sorgfältig zeitnah behoben; vielfach werden die Kunden noch nicht einmal über diese Sicherheitslücken informiert, so dass betroffene Unternehmen Angriffen schutzlos ausgeliefert sind. Also müssten Software- und Hardware-Hersteller auch Adressat des Gesetzes werden. Das kann auf der Grundlage eines deutschen Gesetzes aber nur für Hersteller (oder Vertreiber) in Deutschland gelten. Da die meisten Hersteller ihren Sitz aber im Ausland und nicht einmal in Europa haben, geht die Verpflichtung weitgehend ins Leere.

13 Um die Verpflichtung zur Meldung von Sicherheitslücken wirkungsvoller zu gestalten, müssten für Unternehmen **Anreize und Mehrwert** geschaffen werden, die den potentiellen Reputationsverlust durch das Bekanntwerden des Vorfalls übersteigen. Fehlen diese, besteht die Gefahr einer nur halbherzigen Beteiligung.

14 Insgesamt stellt sich die Frage, ob dieses Gesetz nicht **überflüssig** ist und die Bundesrepublik und insbesondere die Unternehmen der Kritischen Infrastrukturen nicht durch weniger Regulierung und weniger Bürokratie mit der unnützen Verwaltung von Angriffsmeldungen ein höheres Sicherheitsniveau erreichen kann/können.

15 Die **Diktion** sollte insgesamt vereinheitlicht werden: Mal werden nur die 2 Sachziele der Informationssicherheit Integrität, Authentizität genannt, mal werden die 3 (überwiegend anderen!) Sachziele Verfügbarkeit, Integrität, Vertraulichkeit genannt.

Der Gesetzesentwurf findet sich unter:
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile