Bundesministerium des Innern Berlin, den 19. August 2014

Infoblatt IT-Sicherheitsgesetz

Mit der Digitalen Agenda will die Bundesregierung die Digitalisierung von Wirtschaft, Gesellschaft und Staat begleiten und voranbringen. Die Sicherheit der Informationstechnik ist Grundlage jeder Form von Digitalisierung. Sie ist zentrales Querschnittsthema der Digitalen Agenda.

Ein zentrales Vorhaben des Bundesinnenministeriums hierbei ist das IT-Sicherheitsgesetz. Über die im Koalitionsvertrag für ein solches Gesetz vereinbarten Mindestanforderungen an die IT-Sicherheit für Kritische Infrastrukturen und die Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle hinaus nimmt der nun vorliegende Referentenentwurf des Bundesministeriums des Innern die Sicherheit der Systeme und den Schutz der Bürgerinnen und Bürger generell in den Blick. Die IT-Systeme und digitalen Infrastrukturen Deutschlands sollen die sichersten weltweit werden.

Ausgangspunkt für die Konzeption des IT-Sicherheitsgesetzes ist das Verhältnis zwischen Risiko, Schutz und Verantwortung. Wer durch den Einsatz von IT Risiken für andere schafft, hat auch die Verantwortung für den Schutz vor diesen Risiken. Zudem gilt: Je gravierender diese Risiken für unsere Gesellschaft sind, desto höhere Anforderungen sind an die erforderlichen Schutzvorkehrungen zu stellen. Auch wenn das Thema „IT-Sicherheit“ verstärkt global gedacht werden muss: Die Basis hierfür ist ein entschlossenes nationales Handeln.

Der Gesetzentwurf trifft vor diesem Hintergrund Regelungen zu folgenden fünf Themenfeldern:

- Erstes Themenfeld - Verbesserung der IT-Sicherheit bei Unternehmen: Hierzu zählen vor allem Anforderungen an die IT-Sicherheit Kritischer Infrastrukturen mit Mindeststandards und Meldepflichten erheblicher IT-Sicherheitsvorfälle aus dem Koalitionsvertrag von CDU/CSU und SPD.

- Zweites Themenfeld - Schutz der Bürgerinnen und Bürger in einem sicheren Netz:
  Hier sind unter anderem die Erhöhung der Sicherheitsstandards bei öffentlichen Telekommunikationsnetzen und Anbietern von Telemediendiensten sowie die Verpflichtung der Telekommunikationsanbieter zur Information ihrer Kunden über Cyberangriffe und Mittel zu deren Behebung vorgesehen.

- Drittes Themenfeld - Schutz der IT des Bundes:
  Um auch die Bundesregierung selbst stärker in die Pflicht zu nehmen, sieht der Entwurf eine Erweiterung der Möglichkeiten für verbindliche Vorgaben für die IT des Bundes durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor. Hierzu wird die bestehende Regelung für die Regierungsnetze auf die IT des Bundes als Ganzes ausgeweitet.

- Viertes Themenfeld - Stärkung des BSI:
  Der gewachsenen Bedeutung des BSI wird unter anderem durch eine klarere Regelung seiner Warnbefugnisse und seine Etablierung als internationale Zentralstelle Rechnung getragen.

- Fünftes Themenfeld - Zuständigkeitserweiterung BKA:
  Die bestehende Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wird im Bereich der Cyberdelikte ausgeweitet. Gerade bei Angriffen auf bundesweite Einrichtungen ist eine solche klare Zuständigkeitsregelung notwendig.

Der Referentenentwurf des Bundesministeriums des Innern wird nunmehr zunächst innerhalb der Bundesregierung abzustimmen sein und in der Folge intensiv mit den beteiligten Kreisen aus Wirtschaft und Gesellschaft erörtert werden. Bundesinnenminister Dr. de Maizière strebt hierbei ein transparentes Verfahren im Interesse einer breiten öffentlichen Debatte an, die zu maßvollen, wirksamen und sachgerechten Lösungen beiträgt