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

Dr. Katharina Landes **Köln, 23.06.2015**

Der jährliche Bericht zur IT-Sicherheitslage in Deutschland für 2014 hat ergeben, dass die Lage angesichts der Vielzahl neuer Angriffsmethoden und –mittel angespannt ist. Dies zeigt auch der kürzlich erst erfolgte Angriff auf die Systeme des Bundestags. Die fortschreitende Komplexität der IT-Systeme und die stetige Professionalisierung der Cyberangriffe stellen die Betroffenen vor immer neue Herausforderungen.

Um diesen zu begegnen, hat der Bundestag am 12. Juni 2015 ein neues IT-Sicherheitsgesetz beschlossen. Dieses enthält verschiedene Regelungskomplexe, um die IT-Sicherheit in Deutschland zu verbessern. Hier sind insbesondere die folgenden Bereiche zu nennen:

I. Kritische Infrastrukturen

Ein zentrales Vorhaben des Gesetzes ist es, die Anforderungen zu regeln, denen die IT-Sicherheit bestimmter Einrichtungen und Unternehmen standhalten muss. Dabei geht es um sogenannte „Kritische Infrastrukturen“. Kritische Infrastrukturen im Sinne des Gesetzes sind Einrichtungen, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Näheres bestimmt eine Rechtsverordnung des Bundesministeriums des Innern.

→ Betroffen sein werden zum Beispiel Krankenhäuser, Lebensmittelproduzenten, Energie- und Wasserversorger, Banken etc.

Diese Betreiber kritischer Infrastrukturen werden verpflichtet, ein branchenspezifisches Mindestniveau an IT-Sicherheit einzuhalten und mindestens alle zwei Jahre die Erfüllung der Anforderungen durch Sicherheitsaudits oder Zertifizierungen nachzuweisen. Dies bedeutet, dass überall dort organisatorische und technische (ggf. auch infrastrukturelle und personelle) Sicherungsmaßnahmen zu treffen sind, wo die Informationstechnik Einfluss auf die Erbringung der kritischen Dienstleistungen hat. Hauptsächlich werden davon Maßnahmen zur Aufdeckung und Vorbeugung von Störungen erfasst (z.B. Firewall, Angriffserkennungssysteme, Personal-Schulungen etc.), um die Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse zu gewährleisten. Bei besonders kritischen Prozessen kann gegebenenfalls auch eine Abschottung dergestalt erforderlich sein, dass der Prozess weder mit dem Internet oder einem öffentlichen Netz verbunden, noch von einem über das Internet angebotenen Dienst abhängig ist. Maßgeblich ist dabei jeweils der aktuelle Stand der Technik. Den Anforderungen genügen müssen auch Betreiber, die ihre IT durch einen externen Dienstleister betreiben lassen. Um die Umsetzung der Mindestanforderungen zu dokumentieren, wird es als sachgerecht angesehen, diese in entsprechende Sicherheits- und Notfallkonzepte aufzunehmen.

Auftretende IT-Sicherheitsvorfälle sind dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Unterlassen die Unternehmen die Meldung, kann ihnen ein Bußgeld drohen. Die beim BSI zusammenlaufenden Informationen werden ausgewertet und den Unternehmen zur Verbesserung des Schutzes rückgemeldet.

II. Telekommunikations- und Telemediendienste

Zur Steigerung der IT-Sicherheit im Internet werden zudem die Anforderungen an die Anbieter von Telekommunikations- und Telemediendiensten erhöht: Diensteanbieter (z.B. E-Mail-Anbieter, Webseitenbetreiber) haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf ihre technischen Einrichtungen möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen, auch durch äußere Angriffe, gesichert sind. Bei den Sicherheitsmaßnahmen ist von den Anbietern die Einhaltung des Stands der Technik zu gewährleisten, zum Beispiel indem anerkannte Verschlüsselungsverfahren eingesetzt werden.

Zudem sind auch hier auftretende Sicherheitsvorfälle unverzüglich zu melden und die Nutzer über Störungen zu informieren. Für die Überprüfung der Umsetzung ist die Bundesnetzagentur zuständig.

III. Stärkung der Kompetenzen der zuständigen Behörden

Schließlich werden die Kompetenzen des BSI und der Bundesnetzagentur sowie die Ermittlungszuständigkeiten des Bundeskriminalamtes im Bereich der Computerdelikte ausgebaut.

Hinweis

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Klingelhöferstraße 5, 10785 Berlin
Tel. +49 30 884503-0, Fax +49 30 882715-0

HAMBURG
Dammtorstraße 12, 20354 Hamburg
Tel. +49 40 500360-0, Fax +49 40 500360-99

ESSEN
Alfredstraße 220, 45131 Essen
Tel. +49 201 38444-0, Fax +49 201 38444-20

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0, Fax +49 221 33660-80

FRANKFURT AM MAIN
Neue Mainzer Straße 69 – 75, 60311 Frankfurt am Main
Tel. +49 69 170000-17, Fax +49 69 170000-27

MÜNCHEN
Prinzregentenstraße 22, 80538 München
Tel. +49 89 3090667-0, Fax +49 89 3090667-90