Luther.

IP/IT

(Intellectual Property/Information Technology)

Bundestag beschließt IT-Sicherheitsgesetz

Sondernewsletter

Bundestag beschließt IT-Sicherheitsgesetz

Am 12. Juni 2015 hat der Bundestag das IT-Sicherheitsgesetz beschlossen. Durch das neue Gesetz entstehen für Betreiber kritischer Einrichtungen neue Pflichten zur Einführung von Abwehrmaßnahmen, Nachweis- und Meldepflichten.

1. Gegenstand des Gesetzes

Unternehmen in Deutschland sind immer wieder Opfer von Cyberangriffen. Mit Hilfe von USB-Sticks oder Emails wird Schadsoftware in die Unternehmensnetze eingeschleust. Einmal aktiviert, sendet diese Malware Informationen aus den infiltrierten Systemen und kann so bspw. zur Industriespionage genutzt werden. Zudem können Industrieanlagen durch Computerviren gezielt sabotiert werden, indem Steuerungssoftware manipuliert oder die angegriffenen Anlagen physisch beschädigt werden. Cyberangriffe können auf diese Weise insbesondere auch Anlagen und Systeme, die für die Allgemeinheit von erheblicher Bedeutung sind, empfindlich beeinträchtigen. Hierzu zählen etwa Stromnetze, das Gesundheitssystem, die Zahlungssysteme oder die Lebensmittelversorgung. Die Bundesregierung möchte solche kritischen Infrastrukturen deshalb besser als bisher vor den Gefahren von Cyberangriffen schützen.

2. Gesetzgebungsverfahren

Zu diesem Zweck hat die Bundesregierung bereits im März 2013 mit einem Entwurf für ein IT-Sicherheitsgesetz die Diskussion über die Einführung von Maßnahmen zum Schutz gegen Cyberangriffe angestoßen. Der Gesetzesentwurf ist kontrovers diskutiert worden. Kritik äußerten insbesondere IT-Sicherheitsfachleute, Juristen und Datenschützer. Ihre Argumente wurden jedoch nur teilweise im Gesetzestext berücksichtigt.

Der Entwurf wurde am 17. Dezember 2014 von der Bundesregierung beschlossen und dem Bundesrat zugeleitet. Im Bundesrat beschäftigten sich der Ausschuss für innere Angelegenheiten, der Finanzausschuss, der Umweltausschuss und der Wirtschaftsausschuss mit dem Gesetzesvorhaben. Am 6. Februar 2015 gab der Bundesrat eine Stellungnahme ab, in der er das Gesetzesvorhaben insgesamt begrüßte. Der Bundesrat kritisierte dabei etwa die Verwendung von unbestimmten Rechtsbegriffen in vielen wesentlichen Regelungen, wie z. B. „Kritische Infrastrukturen“, „Stand der Technik“ und „erhebliche Störung“.

Die Bundesregierung teilte die Bedenken zur Verfassungsmäßigkeit des Gesetzes nicht. Vielmehr sei es mit Blick auf die Vielschichtigkeit mancher Lebenssachverhalte oftmals unvermeidbar, wertausfüllungsbedürftige Begriffe zu verwenden. Durch eine weitergehende Konkretisierung der Rechtsbegriffe entstünde zudem die Gefahr, dass – in einem insgesamt sehr dynamischen Umfeld – konkrete künftige Entwicklungen nicht mehr erfasst werden könnten. Die Verwendung unbestimmter Rechtsbegriffe mache den Gesetzentwurf demgegenüber zukunfts- und technologieoffen.

Am 27. Februar 2015 wurde der Entwurf für ein IT-Sicherheitsgesetz unverändert dem Bundestag zugeleitet. Der Bundestag hat den Gesetzesentwurf nunmehr mit geringfügigen Änderungen beschlossen.

3. Adressatenkreis

Um den Schutz kritischer Infrastrukturen zu verbessern, sieht der Gesetzesentwurf eine Pflicht zur Einführung von technischen und organisatorischen Mindestmaßnahmen sowie Meldepflichten im Fall von Cyberangriffen vor. Diese Pflichten richten sich an die Betreiber kritischer Infrastrukturen. Allerdings lässt der Gesetzesentwurf offen, wer ein solcher Betreiber einer kritischen Infrastruktur ist. Der Entwurf enthält lediglich zwei Kriterien, anhand derer der Adressatenkreis bestimmt werden soll: Zum einen soll der Adressatenkreis sektorspezifisch eingegrenzt werden und zum anderen durch die möglichen Auswirkungen eines möglichen Cyberangriffs auf die Allgemeinheit. Erfasst sind danach zunächst (nur) die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Zudem sollen Einrichtungen und Anlagen aus diesen Sektoren nur dann als kritische Infrastruktur einzustufen sein, wenn ein Ausfall oder eine Beeinträchtigung dazu führt, dass es zu erheblichen Versorgungsengpässen oder zu einer Gefährdung der öffentlichen Sicherheit kommen könnte.

Da diese abstrakt formulierten Kriterien in der Praxis wenig hilfreich sind, sollen die kritischen Infrastrukturen durch

eine Rechtsverordnung näher bestimmt werden. In dieser Rechtsverordnung sollen qualitative Merkmale sowie Schwellenwerte definiert werden, anhand derer entschieden werden kann, welche Unternehmen von dem Gesetz betroffen sind. Verfassungsrechtlich ist dies kritisch zu bewerten, denn der Gesetzgeber muss grundsätzlich selbst entscheiden, wer von einem Gesetz betroffen ist (Wesentlichkeitstheorie) und kann diese Entscheidung nicht dem Bundesministerium des Innern und damit der ausführenden Gewalt überlassen. Für Unternehmen in den betroffenen Sektoren bedeutet dies jedenfalls, dass erst mit Erlass der Rechtsverordnung eindeutig feststeht, ob sie von den neuen Maßnahmen betroffen sind.

4. Organisatorische und technische Schutzmaßnahmen

Problematisch ist ferner, dass der Gesetzesentwurf nicht festlegt, welche technischen Maßnahmen zukünftig konkret zu ergreifen sind, um kritische Infrastrukturen vor Cyberangriffen zu schützen. Im Gesetzeswortlaut heißt es, dass die Betreiber kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, zu treffen haben.

Welche Maßnahmen angemessen sind, kann von Fall zu Fall unterschiedlich zu beurteilen sein. Bei der Frage der Angemessenheit der Maßnahmen werden die folgenden Kriterien zu berücksichtigen sein: Das Risiko, von einem Cyberangriff betroffen zu werden, die möglichen Auswirkungen eines solchen Angriffs sowie die Kosten der denkbaren technischen Maßnahmen. Weiterhin ist zu beachten, dass die Maßnahmen grundsätzlich dem Stand der Technik entsprechen müssen, so dass ein kontinuierlicher Überprüfungs- und Verbesserungsprozess zu etablieren sein wird.

Erste Vorschläge für konkrete Maßnahmen können der Gesetzesbegründung entnommen werden. Darin wird beispielsweise die Abschottung besonders kritischer Prozesse von den öffentlichen Telekommunikationsnetzen genannt. Zudem finden sich vermehrt Hinweise auf die ISO-Normen, allen voran dem ISO 27001 Standard. Deshalb liegt die Vermutung nahe, dass Betreiber kritischer Infrastrukturen zukünftig ein Informationssicherheitsmanagementsystem (ISMS) einführen und gemäß ISO 27001 zertifizieren müssen.

Diese Empfehlung wird gestützt durch den Entwurf des Sicherheitskatalogs der Bundesnetzagentur (BNetzA), auf den die Gesetzesbegründung für den Energiesektor verweist. In dem Sicherheitskatalog (Entwurf) schreibt die BNetzA für den Energiesektor unter anderem die Einführung eines Informationssicherheitsmanagementsystems gemäß DIN ISO/IEC 27001 sowie die Ernennung eines IT-Sicherheitsbeauftragten vor. Es kann wohl davon ausgegangen werden, dass die von der BNetzA formulierten Anforderungen später auch für die Betreiber kritischer Infrastrukturen in anderen Sektoren (und ggfls. auch Unternehmen außerhalb des eigentlichen Adressatenkreises des Gesetzes) Geltung beanspruchen werden.

Die Betreiber kritischer Infrastrukturen müssen die Mindestmaßnahmen jedoch erst zwei Jahre nach Erlass der Rechtsverordnung eingeführt haben.

5. Nachweispflicht

Die Betreiber kritischer Infrastrukturen müssen mindestens alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen, dass sie ausreichende Schutzmaßnahmen ergriffen haben. Ausweislich der Gesetzesbegründung soll dabei geprüft werden, ob der Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, z. B. ein Information Security Management betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen Besonderheiten umsetzt.

Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen geführt werden. Zudem müssen etwaige Sicherheitsmängel benannt werden. Sollten Sicherheitsmängel aufgetreten sein, kann das BSI umfassendere Informationen, namentlich die vollständigen Prüfberichte, verlangen.

Das Gesetz sieht vor, dass innerhalb der verschiedenen Branchen konkrete Branchenstandards entwickelt werden können, die konkrete Schutzmaßnahmen vorschreiben. Das BSI prüft die Branchenstandards und stellt fest, ob diese ausreichende Sicherheit gewährleisten. Durch Einhaltung eines solchen Branchenstandards können langwierige Einzelfallprüfungen entfallen. Übrigens legt das Gesetz die Anzahl der Standards pro Branche nicht fest, so dass durchaus mehre Branchenstandards vereinbart werden können. Sinnvoll ist es, entsprechende Branchenstandards anhand der Größe der betroffenen Unternehmen zu klassifizieren.

6. Kontaktstelle

Die Betreiber Kritischer Infrastrukturen müssen dem BSI eine Kontaktstelle benennen. Über die Kontaktstelle soll die Kommunikation mit dem BSI geführt werden. Deshalb fordert das Gesetz, dass die Betreiber darüber jederzeit erreichbar sind. Für die Unternehmen bedeutet dies, eine 24/7 Erreichbarkeit sicher zu stellen. Hierfür haben die Betreiber bis sechs Monate nach Inkrafttreten der Rechtsverordnung Zeit.

7. Störungsmeldungen

Kommt es zu einer erheblich Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, und kommt es dadurch zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastruktur, müssen die Betreiber unverzüglich das BSI informieren. Die Information soll über die Kontaktstelle abgesetzt werden.

Die Informationspflicht besteht aber nicht erst dann, wenn die Funktionsfähigkeit der Kritischen Infrastruktur tatsächlich beeinträchtigt ist. Nach dem Grundsatz „Im Zweifel Meldung“ sieht das Gesetz die Informationspflicht bereits dann vor, wenn die Funktionsfähigkeit der Kritischen Infrastruktur beeinträchtigt. Allerdings soll nur bei einer tatsächlichen Störung auch der Betreiber benannt werden. In den anderen Fällen kann die Meldung anonym erfolgen.

8. Datenschutz

Das neue IT-Sicherheitsgesetz verpflichtet Unternehmen zu umfassenden Datenspeicherungen. Allerdings enthält das Gesetz keine Vorgaben zum datenschutzkonformen Umgang, soweit die gespeicherten Daten einen Personenbezug aufweisen, d. h. sich auf die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren Person beziehen. Deshalb wird das Gesetz insbesondere von Datenschützern kritisiert.

Teilweise ist der Gesetzgeber der Kritik nachgekommen. Vor allem wurde der Versuch eine Vorratsdatenspeicherung „durch die Hintertür“ einzuführen, wieder aufgegeben. Geblieben ist jedoch die Berechtigung von Telekommunikationsdiensteanbietern, Bestands- und Verkehrsdaten von Teilnehmern und Nutzern zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Den Telekommunikationsanbietern wird so die Möglichkeit geboten, umfassend Informationen zu speichern, jedoch ohne ein strenge Zweckbindung vorzusehen. Zudem schweigt das Gesetz über die zulässige Höchstspeicherdauer. Aus datenschutzrechtlicher Sicht ist diese Regelung deshalb weiterhin problematisch.

9. Geldbußen

Für den Fall das die Betreiber Kritischer Infrastrukturen keine angemessenen technischen und organisatorischen Maßnahmen zur Vermeidung von Störungen implementieren, kann ein Bußgeld von bis zu EUR 100.000 verhängt werden.

Ebenfalls bußgeldbewährt ist der Fall, dass Sicherheitspannen nicht ordnungsgemäß gemeldet werden. In diesem Fall droht ein Bußgeld von bis zu EUR 50.000.

10. Nächste Schritte

Bis zum Erlass der Rechtsverordnung besteht eine erhebliche Unsicherheit darüber, welche Unternehmen nunmehr als Betreiber Kritischer Infrastrukturen zu klassifizieren sind. Alle Unternehmen, die sich potentiell im Anwendungsbereich des Gesetzes wähnen, sollten jedoch frühzeitig beginnen, die eigenen Schutzmaßnahmen kritisch zu hinterfragen und ggf. zusätzliche Maßnahmen zu ergreifen. Denn sobald die Rechtsverordnung erlassen wird, ist der Umsetzungszeitraum von zwei Jahren, z. B. für die Einführung und Zertifizierung eines ISMS nach ISO 27001, äußert knapp bemessen.

Ferner werden auch Unternehmen außerhalb der betroffenen Sektoren bzw. unterhalb der Schwellwerte mittelbar von den Vorgaben des IT-Sicherheitsgesetzes betroffen sein. Da das Gesetz nur Mindestmaßnahmen vorschreibt, können sich diese Maßnahmen zu einem generellen de facto-Standard weiterentwickeln und auch auf andere Sektoren ausstrahlen. Unternehmen, die massiv von den Vorgaben abweichen, werden dann erklären müssen, warum sie keine vergleichbaren Schutzmaßnahmen ergriffen haben. Eine nur unzureichende Begründung für das Unterlassen angemessener Schutzmaßnahmen kann dann ggf. zu einer Haftung des Unternehmens führen.

Der Bundesrat hat heute angekündigt, am 10. Juli 2015 über das vom Bundestag beschlossene Gesetz beraten zu wollen.

Im Zuge der Aufklärung des Cyberangriffs auf den Bundestag hat die Piratenpartei angekündigt, für das Saarland und Nordrhein-Westfalen einen Entwurf für ein Landes IT-Sicherheitsgesetz einbringen zu wollen.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22
50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Haftungsausschluss

Die Luther Rechtsanwaltsgesellschaft mbH berät in allen Bereichen des Wirtschaftsrechts. Zu den Mandanten zählen mittelständische und große Unternehmen sowie die öffentliche Hand. Die Luther Rechtsanwaltsgesellschaft mbH ist das deutsche Mitglied von Taxand, einem weltweiten Zusammenschluss unabhängiger Steuerberatungsgesellschaften.

Berlin, Brüssel, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Köln, Leipzig,
London, Luxemburg, München, Shanghai, Singapur, Stuttgart

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapore, Yangon

Ihren Ansprechpartner finden Sie auf www.luther-lawfirm.com

Auf den Punkt. Luther.

JUVE 2014 AWARDS
Kanzlei des Jahres
für Regulierte Industrien

JUVE 2014 AWARDS
Kanzlei des Jahres
für Energiewirtschaftsrecht

JUVE 2014 AWARDS
Kanzlei des Jahres
für Privates Baurecht

www.luther-lawfirm.com

Taxand