Luther.

Auf den Punkt. Luther.

Das neue IT-Sicherheitsgesetz

Sinn und Zweck des Gesetzes

Cyberangriffe durch Trojaner, Viren und andere Schadsoftware können Anlagen und Systeme, die für die Allgemeinheit von erheblicher Bedeutung sind, infiltrieren, ausspähen und manipulieren. Der Gesetzgeber möchte deshalb kritische Infrastrukturen wie etwa Stromnetze, die Gesundheits- oder Lebensmittelversorgung sowie Telekommunikationseinrichtungen etc., besser vor den Gefahren von Cyberangriffen schützen.

Adressatenkreis

Verpflichtet sind die Betreiber kritischer Infrastrukturen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Auch Hersteller informationstechnischer Systeme und Zulieferer können betroffen sein.

Konkretisierung durch Rechtsverordnung

Es gibt zwei Kriterien, anhand derer der Adressatenkreis (durch die noch zu erlassende Rechtsverordnung) genauer bestimmt werden soll:

- Qualität: Wird eine für die Gesellschaft kritische Dienstleistung erbracht? Kann also ein Versorgungsengpass oder Gefahren für Leib, Leben, Gesundheit und Eigentum der Bevölkerung drohen?
- Quantität: Ausmaß der Beeinträchtigung (abhängig vom Versorgungsgrad).

Meldepflichten

Das Gesetz legt den Betreibern kritischer Infrastrukturen umfassende Meldepflichten in Bezug auf IT-Sicherheitsvorfälle auf:

- Unverzügliche Meldung im Fall einer Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse.
- Meldung mit Angaben zu der Störung sowie zu den technischen Rahmenbedingungen.
- Einrichtung einer Kontaktstelle mit jederzeitiger Erreichbarkeit.

Organisatorische und technische Maßnahmen

Betreiber kritischer Infrastrukturen müssen technische und organisatorische Maßnahmen ergreifen, um kritische Infrastrukturen vor Cyberangriffen zu schützen. Diese Mindestmaßnahmen müssen innerhalb von zwei Jahren nach Erlass der Rechtsverordnung umgesetzt sein. Hierzu gehören bspw.:

- Einführung von umfassenden Schutzmaßnahmen, etwa Firewalls, Virenscanner, etc.
- Abschottung besonders kritischer Prozesse von öffentlichen Netzen.
- Die Maßnahmen müssen dem aktuellen Stand der Technik entsprechen.
- Branchenstandards können konkrete Schutzmaßnahmen enthalten.

Regulierte Branchen und „Best Practices“

In bestimmten Branchen, wie etwa dem Energiesektor oder der Telekommunikation, gibt es schon Standards oder Vorgaben der zuständigen Behörde (BNetzA). So enthält bspw. auch der Entwurf der Bundesnetzagentur für einen Sicherheitskatalog gemäß § 11 Abs. 1 a EnWG konkrete Hinweise für gebotene Maßnahmen. Dort wird u.a. gefordert, künftig ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO 27001 einzuführen und aufrechtzuerhalten. Das legt die Vermutung nahe, dass künftig alle Betreiber kritischer Infrastrukturen zur Erfüllung der geforderten Maßnahmen und Einhaltung einschlägiger Standards ein ISMS einführen und zertifizieren sollten.

Sonstige Pflichten

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. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen geführt werden.

Geldbußen und Haftung

- Bei fehlenden angemessenen technischen und organisatorischen Maßnahmen beträgt das Bußgeld bis zu EUR 100.000.
- Bei nicht ordnungsgemäßer Meldung von Sicherheitspannen beträgt das Bußgeld bis zu EUR 50.000.
- Daneben treffen die Geschäftsführung Sorgfaltspflichten bei der Etablierung und Aufrechterhaltung von IT-Security im Unternehmen.

Inkrafttreten

Das neue IT-Sicherheitsgesetz wird voraussichtlich im August 2015 in Kraft treten.

Ihre Ansprechpartner

Dr. Michael Rath
Rechtsanwalt, Fachanwalt für IT-Recht, Partner
michael.rath@luther-lawfirm.com
Telefon +49 221 9937 25795

Christian Kuß, LL.M.
Rechtsanwalt
christian.kuss@luther-lawfirm.com
Telefon +49 221 9937 25711

Auf den Punkt.

- **Verbesserung der IT-Sicherheit bei Unternehmen durch Verpflichtung zur Einführung technischer und organisatorischer Schutzmaßnahmen**
- **Etablierung verbindlicher Mindeststandards zur IT-Sicherheit für die einzelnen Branchen**
- **Verbindliche Meldepflichten bei vermuteten und tatsächlichen Eingriffen in die IT-Infrastruktur**
- **Einrichtung einer Kontaktstelle (24/7) zur Kommunikation mit dem BSI**
- **Bei Verstößen drohen Geldbußen bis EUR 100.000**

Save the date

Veranstaltung „IT-Sicherheit und Datenschutz“ am 25. August 2015 in Köln

Luther Rechtsanwaltsgesellschaft mbH,
Anna-Schneider-Steig 22, 50678 Köln

Erfahren Sie mehr!