Wer ist vom IT-Sicherheitsgesetz betroffen?

Ein Beitrag von Miriam Schuh

Die BSI-Kritisverordnung definiert, welche Unternehmen von den Pflichten des IT-Sicherheitsgesetzes betroffen sind

Hintergrund

Aufgrund des seit Juli 2015 geltenden Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) obliegen Betreibern von „kritischen Infrastrukturen" bestimmte Pflichten zur Sicherheit ihrer Systeme. Hierzu gehört insbesondere die Einhaltung eines IT-Mindestsicherheitsniveaus. Zudem sind die Betreiber verpflichtet, erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Problematisch war bisher, dass der Begriff der „kritischen Infrastruktur" im IT-Sicherheitsgesetz nicht abschließend legal definiert wurde. Dies erschwerte die Einschätzung, wer als Betreiber von Anlagen unter die Bestimmungen des IT-Sicherheitsgesetzes galt und die damit einhergehenden Pflichten zu erfüllen hatte und führte zur Rechtsunsicherheit.

Aktuelle Änderung

Mit der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) definiert der Gesetzgeber nunmehr die „kritischen Infrastrukturen", indem er die darunter fallenden Anlagen abschließend auflistet. Bereits im Mai 2016 trat der erste Teil der Verordnung in Kraft, mit dem geregelt wurde, welche Anlagen in den Sektoren Energie, Wasser, Ernährung und Informationstechnik und Telekommunikation als „kritische Infrastrukturen" gelten. Am 31.05.2017 wurde mit der ersten Verordnung zur Änderung der BSI-KritisV nun auch dem zweiten und abschließenden Teil der Verordnung durch die Bundesregierung zugestimmt. Auf deren Basis kann nun auch im Detail bestimmt werden, welche Anlagen in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr als kritische Infrastrukturen einzustufen sind, so dass Unternehmen nunmehr rechtssicher beurteilen können, ob Sie unter die Anwendbarkeit des IT-Sicherheitsgesetzes fallen oder nicht.

Praktische Auswirkungen: Compliance-Check nach IT-Sicherheitsgesetz!

Für in den genannten Branchen tätige Unternehmen gilt es somit zu prüfen, ob sie in den Anwendungsbereich des IT-Sicherheitsgesetzes fallen. Trifft das zu, müssen innerhalb von zwei Jahren, nach Inkrafttreten der ersten Verordnung zur Änderung der BSI-KritisV (voraussichtlich noch im Juni 2017), innerhalb der betroffenen Unternehmen erhöhte Sicherheitsstandards umgesetzt werden. Das IT-Sicherheitsgesetz betrifft unmittelbar Anlagenbetreiber. Mittelbar werden aber auch Hersteller von Anlagen oder Anlagenteilen die Auswirkungen des Gesetzes spüren, da die Betreiber zur Konformität ihrer Sicherheitssysteme die Mitwirkung der Hersteller benötigen und diese dazu in ihre Informationssicherheitsmanagementsysteme einbinden müssen.

Die Hersteller haben in diesem Rahmen die Sorge für die ordnungsgemäße die Bereitstellung aller - für das entsprechend verpflichtende Sicherheitsniveau - notwendigen Produktinformationen zu tragen.
Hersteller sollten daher Strukturen implementieren, um sich zunächst mit ihren Kunden in Verbindung zu setzen und zu prüfen, ob diese Betreiber der im IT-Sicherheitsgesetzt bezeichneten Anlagen sind. Gleichzeitig ist zu prüfen, ob dem Hersteller eine erhöhte Informationspflicht zukommt und die erforderlichen Informationen umfassend eingeholt und an die Kunden übermittelt werden können.

Unternehmenskontakt: Melanie Schuh / Head of Marketing & Communications / T +49 30 2332895-0 / E melanie.schuh@reuschlaw.de