Aktuell

Neues aus der IT-Beratung

Betreiber kritischer Infrastrukturen - Auch der Mittelstand gehört dazu

Betreiber kritischer Infrastrukturen sind dazu verpflichtet, die Erfüllung der Anforderungen aus § 8a (1) BSIG gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu belegen. Stichtag für die Erbringung dieses Nachweises war der 3. Mai 2018.

Mit dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist ein verbindlicher normativer Rahmen erlassen worden, der dazu dienen soll, die IT-Systeme und digitalen Geschäftsprozesse von Betreibern sogenannter „kritischer Infrastrukturen" sicherer zu gestalten. Diese Maßnahme soll sicherstellen, dass die Grundversorgung der Bevölkerung mit wichtigen Versorgungsgütern nicht durch den Ausfall zentraler IT-Systeme wesentlich beeinträchtigt wird. Nach § 8a BSIG müssen Betreiber kritischer Infrastrukturen die Einhaltung eines angemessenen IT-Sicherheitsniveaus nach dem Stand der Technik regelmäßig gegenüber dem BSI nachweisen. Das BSI erhielt die Befugnis, in einer Rechtsverordnung (BSI-Kritis-Verordnung; nachfolgend BSI-KritisV) genauer zu definieren, nach welchen Kriterien ein Unternehmen als Betreiber kritischer Infrastruktur eingestuft wird.

Wer sind Betreiber kritischer Infrastrukturen? – In der BSI-KritisV wurde festgelegt, welche Branchen grundsätzlich als Betreiber kritischer Infrastrukturen eingestuft werden und ab welchem Schwellwert (z.B. Anzahl versorgter Haushalte, abgesetzte Produktmenge) diese einer Nachweispflicht gegenüber dem BSI unterliegen. Betreiber kritischer Infrastrukturen können beispielsweise Unternehmen aus den Sektoren: Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr sein, sofern sie den definierten Schwellenwert überschreiten. Auch mittelständische Unternehmen überschreiten mitunter die definierten Schwellenwerte und sind somit dazu verpflichtet, einen Nachweis gegenüber dem BSI zu erbringen.

Prüfungspflicht und Nachweis – Für die Erbringung eines Nachweises müssen die IT-Systeme des Unternehmens durch eine sogenannte „prüfende Stelle" auditiert werden. Dieses kann u.a. durch qualifizierte Wirtschaftsprüfungsgesellschaften erfolgen.

Prüfgrundlage – Als möglicher Bewertungsmaßstab wurden - vom BSI freizugebende - branchenspezifische Sicherheitsstandards (sog. B3S) zugelassen sowie Audits und Zertifizierungen auf der Grundlage einschlägiger Standards (z.B. Zertifizierungsschemata für ISO 27001 nativ - oder auf Basis von IT-Grundschutz).

Sprechen Sie uns an:

Gerne stehen wir Ihnen zur Verfügung, um zu ermitteln, ob auch Ihr Unternehmen als Betreiber einer kritischen Infrastruktur eingestuft werden könnte. Wir können Sie bei der Auswahl und Einrichtung geeigneter Sicherheitsmaßnahmen unterstützen und die Auditierung gegenüber dem BSI für Sie vornehmen.

Ihr Kontakt zu diesem Thema: Kira Zucher · zucher@treuhand.de