# Bundestag verabschiedet IT-Sicherheitsgesetz

*Jetzt ist es so weit. Der Deutsche Bundestag hat das IT-Sicherheitsgesetz beschlossen. Was bedeutet dies jetzt für Ihr Unternehmen? Das Gesetz können Sie verteilt auf die zwei Drucksachen des Bundestages 18/4096 (Entwurf) und 18/5121 (letzte Änderungen) herunterladen und sich im Zusammenhang mit den dadurch geänderten Gesetze zu Gemüte führen. Hier ein kurzer Abriss zu den wichtigsten Konsequenzen*

## Allgemeines

Mit der Verabschiedung des Gesetzes reagiert die Bundesregierung auf die derzeit in allen Medien zu verfolgende angespannte Sicherheitslage im Bereich der IT. Ganz besonders werden durch das Gesetz bundesweit etwa 2000 Betreiber sogenannter kritischer Infrastrukturen angesprochen. Aber auch andere Unternehmen aus den Sektoren Energie, Telekommunikation oder Betreiber von Telemediendiensten werden angesprochen.

So will das neue Gesetz im Besonderen dafür sorgen, dass die IT- bzw. Informationssicherheit in allen Bereichen befördert wird. So verlangt das Gesetz von zahlreichen Branchen IT-Sicherheitsmaßnahmen nach dem Stand der Technik sowie die Einrichtung von Verfahren um bei Störfällen diese der BNetzA und/oder ihren Nutzern zu melden. Energieversorger müssen darüber hinaus eine Zertifizierung nach ISO/IEC 27001 durchführen. Private IT-Nutzer sind von den Auswirkungen des Gesetzes ausgenommen.

## KRITIS

Die unter Begriff KRITIS zusammengefassten kritischen Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." Oder wie es ein BSI Vertreter kürzlich in einem Workshop ausgedrückt hat: "Infrastrukturen bei deren Ausfall Unruhen bis hin zu einem Bürgerkrieg drohen könnte". Diese Unternehmen sind am stärksten hinsichtlich Meldepflicht von Ereignissen und Maßnahmen zum Nachweis der IT-Sicherheit betroffen. Nach Auskunft des BSI zählen dazu die 2000 wichtigsten Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen.

Sofern Ihr Unternehmen nicht dazu zählt, können Sie die Ausführungen zu KRITIS getrost überlesen. Anderenfalls stehe ich Ihnen gerne im Rahmen eines Beratungsgespräches zu Verfügung die Auswirkungen auf Ihr Unternehmen zu diskutieren.

## Energieversorger

Durch die Änderung des Energiewirtschaftsgesetzes durch Artikel 3 des Gesetzes gelten für Energieversorger besondere Bedingungen. So müssen Sie die Anforderungen des derzeit noch im Entwurf

befindlichen IT-Sicherheitskatalogs der BNetzA erfüllen. Dieser erfordert im Besonderen eine Informationssicherheitszertifizierung ihrer Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, nach der internationalen Norm ISO/IEC 27001 mit den branchenspezifischen Ergänzungen ISO/IEC 27019

## Anbieter von Telemedien-Dienstleistungen

Heutzutage betreibt nahezu jede Firma eine Website und unterliegt damit dem Telemediengesetz. Damit muss sie nach Artikel 4 des Gesetzes in Zukunft sicherstellen, dass, soweit dies technisch möglich und wirtschaftlich zumutbar ist und dem Stand der Technik entspricht, kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist. Gleiches gilt auch für den Schutz personenbezogener Daten und Schutz vor Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

Erfrischend, dass der Gesetzgeber hier mit der Formulierung "soweit dies technisch möglich und wirtschaftlich zumutbar ist" ausdrücklich nichts Unsinniges oder Unmögliches fordert☺.

## Telekommunikationsanbieter

Artikel 5 des IT-Sicherheitsgesetztes beschreibt schließlich die Änderungen an dem Telekommunikationsgesetz.

- Anbieter von Telekommunikationsdiensten dürfen jetzt ausdrücklich Verkehrs- und Bestandsdaten verwenden um Störungen der IT-Sicherheit (Hacker) innerhalb ihrer Systeme zu beheben.
- War bisher nur ein Sicherheitskonzept von dem Betreiber gefordert, das die BNetzA überprüfen konnte, soll nun die Überprüfung regelmäßig alle 2 Jahre erfolgen.
- Die Meldepflicht umfasst nach dem neuen Gesetz jetzt auch Beeinträchtigungen, die zu erheblichen Sicherheitsverletzungen führen können. Es muss also noch nichts „passiert“ sein.
- Gehen von einer Datenverarbeitungseinrichtung eines Nutzers Störungen aus (Virus, Botnetz) so ist der Dienstanbieter nun verpflichtet den Nutzer darauf hinzuweisen und ihm auf technische Mittel hinweisen um diese Störung zu beseitigen.

## Sonstiges

Sollten Sie noch Fragen zu dem Themenkomplex haben stehe ich Ihnen gerne für Nachfragen zur Verfügung. Gerne schicke Ich Ihnen auf Anfrage die oben zitierten Dokumente so weit möglich zu.

## Kontakt

Falls Sie noch Fragen zu dem Thema haben, freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de
ISO 27001 Auditor, externer Datenschutzbeauftragter