/ IT-Sicherheitsgesetz 2.0: Neue Anforderungen und erweiterter Adressatenkreis

07.06.2021

Digital Business | IT & Outsourcing | Datenschutz | Brüssel

Am 23.04.2021 hat der Deutsche Bundestag das „IT-Sicherheitsgesetz 2.0“ beschlossen. Nachdem nun auch der Bundesrat am 07.05.2021 zugestimmt hat, ist das Gesetz am 28.05.2021 in Kraft getreten (BGBl 2021 Teil I Nr. 25).

Mit weitreichenden Änderungen in einer ganzen Reihe von Einzelgesetzen (insb. BSI-Gesetz, Energiewirtschaftsgesetz, Telemediengesetz, Telekommunikationsgesetz, BKA-Gesetz) war das Gesetzesvorhaben von Anfang an sehr umstritten. Während des Gesetzgebungsverfahrens wurden zahlreiche Referentenentwürfe präsentiert und neugefasst. Begleitet wurde das Verfahren von teilweise massiver Kritik seitens Netzaktivisten, Verbänden und Experten, die insbesondere aufgrund erweiterter Eingriffsbefugnisse (z.B. Portscans) einen Umbau des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur „Hackerbehörde“ befürchten.

Wesentliche Inhalte der Reform

Das Gesetz soll die rechtlichen Grundlagen der „Cyber-Sicherheitsstrategie“ der Bundesregierung schaffen und die Informationssicherheit in Deutschland verbessern. Dies geht mit einem massiven personellen Ausbau des BSI einher, das mit insgesamt 799 neuen Stellen erweitert werden soll. Im Wesentlichen verfolgt das Gesetz insbesondere vier Ziele:

- Stärkung der Rolle des BSI
- Inhaltliche Erweiterung von Pflichten für Betreiber kritischer Infrastrukturen und weiterer Unternehmen im besonderen öffentlichen Interesse
- Einführung eines einheitlichen IT-Sicherheitskennzeichens zum Schutz von Verbrauchern
- Stärkung der staatlichen Schutzfunktion

Ausweitung des Anwendungsbereichs auf „Unternehmen im besonderen öffentlichen Interesse“

Das Gesetz sieht nunmehr spezielle Pflichten auch für „Unternehmen im besonderen öffentlichen Interesse“ vor. Hierunter fallen zunächst Unternehmen, die nach Ansicht des Gesetzgebers von „erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind“ (vgl. § 2 Abs. 14 S. 1 Nr. 2 BSI-Gesetz neu). Eine vom Bundesministerium für Inneres, Bau und Heimat noch zu erlassene Verordnung soll diesen Begriff näher präzisieren und genaue Schwellenwerte festlegen (vgl. § 10 Abs. 5 BSI-Gesetz neu). Damit verabschiedet sich der Gesetzgeber ein Stück weit von der bis dato vorherrschenden Systematik des IT-Sicherheitsrechts und weitet dessen Anwendungsbereich aus. Während sich der Anwendungsbereich des BSI-Gesetzes bisher vor allem nach der Zugehörigkeit eines Unternehmens zu einem bestimmten Sektor bestimmte, betrifft die Regulierung nun grundsätzlich alle Unternehmen ab einer bestimmten Wichtigkeit für die deutsche Volkswirtschaft. Dies gilt insbesondere auch für Zulieferer (vgl. § 2 Abs. 14 S. 1 Nr. 2 BSI-Gesetz neu). Auch Unternehmen, die keinem der in § 2 Abs. 10 BSI-Gesetz aufgezählten Sektoren angehören, sollten daher genau prüfen, ob sich für sie aus dem IT-Sicherheitsgesetz 2.0 (neue) Pflichten ergeben können.

Die gesetzlichen Anforderungen für Betreiber kritischer Infrastrukturen werden nunmehr auch auf den Sektor der „Siedlungsabfallentsorgung“ ausgedehnt (§ 2 Abs. 10 BSI-Gesetz neu). Damit zählen auch Entsorger ab bestimmten Schwellenwerten zur kritischen Infrastruktur. Es ist davon auszugehen, dass im Zuge des IT-Sicherheitsgesetzes 2.0 auch eine

Novellierung der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erfolgen wird, in der unter anderem genaue Schwellenwerte festgelegt werden.

Erweiterte Pflichten für Betreiber kritischer Infrastrukturen

Auch inhaltlich wird das Pflichtenspektrum des BSI-Gesetzes erweitert.

Betreiber kritischer Infrastrukturen sind nunmehr verpflichtet, sich *unmittelbar* beim BSI zu registrieren (vgl. § 8b Abs. 3 S. 1 BSI-Gesetz neu). Zudem müssen sie ab dem 01.05.2023 „Systeme zur Angriffserkennung" verwenden (§ 8a Abs. 1a BSI-Gesetz neu).

Zudem müssen Betreiber kritischer Infrastrukturen nun den geplanten erstmaligen Einsatz von „kritischen Komponenten" dem Bundesministerium des Innern, für Bau und Heimat anzeigen (§ 9b Abs. 1 S. 1 BSI-Gesetz neu). Der über § 2 Abs. 13 S. 1 Nr. 2 BSI-Gesetz neu eingeführte Begriff der „kritischen Komponenten" meint bestimmte IT-Produkte, die für die Funktionsfähigkeit kritischer Infrastrukturen besonders wichtig sind oder die öffentliche Sicherheit potentiell gefährden können. Auch eine Untersagung des Einsatzes solcher kritischer Komponenten durch das Bundesministerium für Inneres, Bau und Heimat ist nun möglich (vgl. § 9b Abs. S. 1 BSI-Gesetz neu), etwa wenn der Hersteller der Komponente von einem Drittstaat kontrolliert wird oder den „sicherheitspolitischen Zielen" der Bundesregierung, EU oder Nato widerspricht. Diese Regelung wurde in der medialen Berichterstattung intensiv unter dem Begleitnamen „Lex Huawei" diskutiert. Unternehmen sollten ihre eingesetzten IT-Produkte darauf überprüfen, ob sie nun Anzeigepflichten und etwaige Untersagungsrisiken treffen und sich gegebenenfalls mit technischen Alternativen befassen.

Für „Unternehmen im besonderen öffentlichen Interesse" sieht das Gesetz die Pflicht zur Abgabe einer Selbsterklärung vor, mit der sie darlegen müssen, welche Zertifizierungen im Bereich der IT-Sicherheit sie in den letzten zwei Jahren durchgeführt haben und wie ihre IT-Systeme geschützt sind (§ 8f Abs. 1 BSI-Gesetz neu).

Unternehmen sollten das Thema IT-Sicherheit auf jeden Fall im Auge behalten. Das legt nicht nur der stetige Anstieg an Cyberangriffen nahe. Das BSI verzeichnete für 2020 einen durchschnittlichen Zuwachs von rund 322.000 neuen Computervirus-Varianten pro Tag. Auch die rechtlichen Implikationen von IT-Sicherheitsvorfällen sind nicht zu unterschätzen. Das neue IT-Sicherheitsgesetz 2.0 sieht Bußgelder in Höhe von bis zu 20 Millionen Euro vor (§ 14 Abs. 5 S. 1 BSI-Gesetz neu, § 30 Abs. 2 S. 3 OWiG).

Update Datenschutzrecht

Auch aus datenschutzrechtlicher Sicht enthält das IT-Sicherheitsgesetz eine Reihe interessanter Neuerungen. Das BSI darf künftig Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen – etwa im Rahmen der Kommunikation zwischen Bürger und Behörde – bis zu 18 Monate speichern. Zudem kann die Behörde im Falle einer Störung von den Betreibern kritischer Infrastrukturen die Herausgabe notwendiger Informationen einschließlich personenbezogener Daten verlangen (§ 8b Abs. 4a BSI-Gesetz neu).

Ausblick: Reform der Europäischen NIS-Richtlinie

Das Thema IT-Sicherheit steht nicht nur auf nationaler Ebene im Fokus. Auch bei der Europäischen Union hat die Sicherstellung der Cybersecurity hohe Priorität. In Sachen IT-Sicherheit setzte der europäische Gesetzgeber mit der NIS-Richtlinie ((EU) 2016/1148 , umgesetzt vor allem im aktuellen BSIG) erstmals Maßstäbe für die gesamte EU. Vier Jahre danach will der Europäische Gesetzgeber die NIS-Richtlinie gründlich überarbeiten. Der Vorschlag der Europäischen Kommission einer NIS 2.0 (COM(2020) 823 final), der Teil der neuen Cybersicherheitsstrategie ist, enthält umfangreiche Anpassungen und Änderungen. Ergänzend hat die Europäische Kommission eine „Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen" vorgelegt, die ebenfalls Onlinerisiken adressiert. Es ist also durchaus möglich, dass die Regelungen des neuen IT-Sicherheitsgesetzes 2.0 im

Rahmen der Umsetzung der europäischen Richtlinien schon bald wieder überarbeitet werden müssen.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Daniel Rücker , Dr. David Bomhard oder Andreas Daum
Praxisgruppen: Digital Business , IT & Outsourcing , Datenschutz

Contact Person

Dr. Daniel Rücker, LL.M.
Leiter Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457

Dr. David Bomhard
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628 2610

Andreas Daum, LL.M. (LSE)
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628 466