Herausforderungen des neuen *BSI-Gesetzes*:
Cyber-Sicherheit wird für viele Unternehmen zum Pflichtprogramm

Cyber-Sicherheit rückt erneut in den Fokus des Gesetzgebers. Nach dem Ausfall ganzer Universitäten und Kliniken in Deutschland sowie der Treibstoff-Versorgung in den USA sollen kritische Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse verstärkt in die Pflicht genommen werden. Dafür sorgt nun das neue IT-Sicherheitsgesetz 2.0 und die dritte KRITIS-Verordnung.

Dreh- und Angelpunkte der Änderungen sind die Stärkung des Bundesamtes für Sicherheit in der Informationstechnik („**BSI**“) im BSI-Gesetz („**BSIG**“) sowie erhebliche Erweiterungen im Kreis der Verpflichteten.

Auch der Verbraucherschutz gehört fortan zu den Aufgaben des BSI. Ein neues **IT-Sicherheitskennzeichen für Verbraucher** soll erkennbar machen, ob ein Produkt einschlägige IT-Sicherheitsstandards einhält. Zudem soll das BSI in Zukunft bei verpflichteten Unternehmen **Portscans an Schnittstellen zu öffentlichen Telekommunikationsnetzen** durchführen dürfen.

Unternehmen müssen bereits jetzt prüfen, welche Auswirkungen die Änderungen auf sie haben können, denn anders als bei vorherigen Änderungen gibt es keine Schon- oder Übergangsfrist und Verstöße können nun zu empfindlichen Bußgeldern von bis zu EUR 2 Millionen führen.

Unternehmen sollten jetzt klären, ob:

- sie in den erweiterten Verpflichtetenkreis fallen - insbesondere als KRITIS oder UNBÖFI - und welche Anforderungen an IT-Sicherheitscompliance sie erfüllen müssen;
- sie kritische IT-Komponente einsetzen, die möglicherweise gegenüber dem BMI anzuzeigen sind;
- es Handlungsbedarf im Hinblick auf Zulieferer / in der Lieferkette gibt;
- bereits bestehende Prozesse für die IT-Sicherheitscompliance verwendet werden können - insbesondere aus dem Datenschutz - oder ob neue Prozesse aufgestellt werden müssen; und ob
- ein IT-Sicherheitszertifikat erforderlich wird.

Wir stellen im Folgenden (1) den Hintergrund und die wichtigsten Änderungen im Überblick dar. Anschließend werfen wir einen genaueren Blick auf (2) die Änderungen bei den Verpflichteten sowie (3) im Bereich Produktsicherheit und kritische Komponenten. (4) Abschließend widmen wir uns der ausgeweiteten Kompetenz des BSI zur Gefahrenabwehr und Marktüberwachung im digitalen Bereich.

1. Hintergrund und Anwendungsbereich des BSIG

Grundlage für die Bekämpfung **IT-spezifischer Gefahren** wie Cyberangriffe und Sicherheitsvorfälle ist die Cyber-Sicherheitsstrategie für Deutschland, die Digitale Agenda der Bundesregierung und die NIS-Richtlinie der EU (RL EU 2016/1148). Verkörperung fanden

diese Grundlagen in dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI-Gesetz oder BSIG.

Das BSIG weist dem **BSI als zentrale Cybersicherheits-Behörde** die zur Sicherstellung der IT-Sicherheit notwendigen Aufgaben und Befugnisse sowohl gegenüber Stellen des Bundes als auch gegenüber privaten Unternehmen zu. Die Aufgaben und Befugnisse sind vielfältig und zielen insgesamt darauf ab, die **Funktionsfähigkeit von IT-Systemen** der für den Staat oder das Funktionieren des öffentlichen Lebens kritischen Systeme sicherzustellen.

So sind **Betreiber kritischer Infrastrukturen („KRITIS“)** verpflichtet, technische und organisatorische Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Hierzu gehören auch Systeme zur Angriffserkennung. Die Umsetzung dieser Maßnahmen müssen sie **gegenüber dem BSI nachweisen.** Bei eingetretenen oder befürchteten Sicherheitsvorfällen besteht eine **unverzügliche Meldepflicht**.

Entsprechendes gilt auch für Anbieter relevanter **digitaler Dienste**, worunter Anbieter von Suchmaschinen, Online-Marktplätzen oder Cloud-Computing- sowie Telemedien-Diensten fallen.

2. Die neuen Verpflichteten

Die Neuerungen im IT Sicherheitsrecht sollen vor allem den **Kreis der Verpflichteten vergrößern**. Zentral bleibt zunächst weiterhin der Begriff KRITIS. Dieser soll durch eine Kategorie erweitert werden: die **Siedlungsabfallentsorgung**. Hier wird eine Verordnung den Umfang der Kategorie noch näher bezeichnen.

Die bereits festgelegten und näher bestimmten KRITIS-Kategorien werden durch eine zweite Änderungsverordnung weiter ausgeweitet: Bisher erfasste das BSIG ca. 1600 Betreiber kritischer Infrastruktur. Durch **Änderungen** in den jeweiligen **Bemessungskriterien und Schwellenwerten** sollen hier nun geschätzte **270 weitere Betreiber** hinzukommen.

Neben KRITIS soll darüber hinaus ein gänzlich neuer Bereich in den Pflichtenkatalog des BSIG aufgenommen werden: Dafür gibt es nun den neuen Begriff des **Unternehmens im besonderen öffentlichen Interesse** („**UNBÖFI**“). Der Gesetzgeber will damit der Tatsache Rechnung tragen, dass die IT-Sicherheit entscheidender deutscher Wirtschaftsakteure auch dann von zentraler Bedeutung ist, wenn diese keine kritische Infrastruktur bedienen. UNBÖFIs sind im Wesentlichen drei Arten von Unternehmen – einschließlich **zentraler Zulieferer**:

- **IT-Sicherheitsprodukthersteller** sind Hersteller oder Entwickler von Gütern im Sinne des § 60 I Nr. 1, 3 AußenwirtschaftsVO. Dies umfasst Unternehmen, die
  - Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder
  - für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellen, oder hergestellt haben und noch über die dabei zugrundeliegende Technik verfügen

  und deren Produkte oder im Falle für die IT-Sicherheitsfunktion wesentlicher Komponente das Gesamtprodukt vom BSI zugelassen wurden.

- **Kritische Betreiber nach dem BImSchG** (Bundesimmissionsschutzgesetz) sind solche Betreiber, welche in einen Betriebsbereich der oberen Klasse nach der 12. BImSchV

(der Störfall-Verordnung) fallen, sowie die denen in der Verordnung gleichgesetzten Betreiber eines Betriebsbereichs der unteren Klassen, also Betreiber, in deren Betrieben als gefährlich ausgewiesene Stoffe in Mengen vorhanden sind, welche die in der Verordnung angegebenen Mengenschwellen erreichen oder überschreiten.

- **Unternehmen von erheblicher volkswirtschaftlicher Bedeutung** sind Unternehmen, welche nach inländischer Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik sind. Welche Unternehmen hiervon genau erfasst sind, muss durch eine weitere Verordnung zunächst festgelegt werden. Ein Indiz für eine mögliche Auflistung gibt das s.g. Hauptgutachten der Monopolkommission, welches die nach inländischer Wertschöpfung 100 größten Unternehmen im jeweiligen Berichtsjahr auflistet. Das aktuelle Gutachten kann hier eingesehen werden, die Auflistung für das Berichtsjahr 2018 findet sich in den Tabellen zum Kapitel II.

- **Zulieferer der Unternehmen von erheblicher volkswirtschaftlicher Bedeutung**, welche wegen ihrer **Alleinstellungsmerkmale** von wesentlicher Bedeutung sind. Was unter Alleinstellungsmerkmal zu verstehen ist, soll durch eine Verordnung festgelegt werden.

3. ***Produktsicherheit und kritische Komponenten***

Mit dem IT-Sicherheitsgesetz 2.0 schreitet die **Digitalisierung des Produktrechts** voran.

IT-Sicherheitskennzeichen

Eingeführt wird ein **freiwilliges IT-Sicherheitskennzeichen** zur Information von Verbrauchern, welches Unternehmen u. a. für Vermarktungszwecke nutzen können. Hierfür wird das BSI zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom BSI festgelegter Produktkategorien ein einheitliches Kennzeichen einführen. Das Kennzeichen dürfte v. a. für ausländische Unternehmen interessant sein, um deutsche Verbraucher davon zu überzeugen, dass das IT-Produkt deutschen Sicherheitsstandards entspricht.

In Umsetzung europäischen Rechts werden die geplanten Änderungen des Bürgerlichen Gesetzbuchs (BGB) im Fall einer Bereitstellung digitaler Produkte an Verbrauchern eine Update-Verpflichtung des vertreibenden Unternehmens begründen.

Eingriffsbefugnisse des BSI

Weitere Änderungen betreffen die Schaffung von Eingriffsbefugnissen des BSI für den Einsatz und Betrieb von **kritischen Komponenten**. Mit einer Regelung zur Untersagung des Einsatzes solcher Komponenten von nicht vertrauenswürdigen Herstellern soll die Produktsicherheit im Bereich der kritischen Infrastrukturen erhöht werden.

Erfasst wird sowohl Hard- als auch Software, die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit des IT-Produkts zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können.

Die neuen Anforderungen für kritische Komponenten sind eng mit dem neuen **Telekommunikationsgesetz** verzahnt. Für weitere Details verweisen wir auf unseren Client Alert zum Telekommunikationsmodernisierungsgesetz.

4. ***Im digitalen Bereich: Gefahrenabwehr- und Marktüberwachung durch das BSI – Pflichten für Unternehmen***

Das geänderte BSIG dient des Weiteren dazu, in Anbetracht eines stetigen Zuwachses an IT-Schadprogrammen Schutzmechanismen und Abwehrstrategien anzupassen. Konkret sieht es daher eine Verbesserung des Schutzes der auf den Markt bereitgestellten IT-Produkte und Systeme unter anderem durch weitere Prüf- und Kontrollbefugnisse des BSI und Festlegung von Mindeststandards vor:

- Das BSI erhält die Befugnisse zur Detektion von Schadprogrammen. So darf das BSI durch sogenannte „*Portscans*“ ermitteln, ob Betreiber öffentlich erreichbarer informationstechnischer Systeme dem BSI bekannt gewordene Sicherheitslücken geschlossen haben.
- Werden dem BSI Sicherheitslücken oder -risiken bekannt, die von Telekommunikations- oder Telemediendiensten ausgehen, kann die Behörde gegenüber den Anbietern solcher Dienste Maßnahmen anordnen, um die Risiken zu beseitigen (z.B. ein Software-Update).

Mit dem IT Sicherheitsgesetz 2.0 erhält das BSI zudem weitreichende Anordnungsbefugnisse gegenüber Telekommunikations- und Telemedienanbietern, um spezifische Gefahren für die Informationssicherheit abzuwehren. Gleichzeitig werden auch die Pflichten für Unternehmen ausgeweitet.