



Update Recht:  
IT-Sicherheitsgesetz  
veröffentlicht

Mai 2021

## Update Recht: IT-Sicherheitsgesetz veröffentlicht

*Das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ wurde vom Bundestag am 23.4.2021 verabschiedet, vom Bundesrat am 7.5.2021 gebilligt und am 27.5.2021 veröffentlicht. Wir haben uns das IT-Sicherheitsgesetz genauer angeschaut und hier für Sie zusammengefasst.*

Die meisten Vorschriften des IT-Sicherheitsgesetzes treten dabei bereits direkt in Kraft; ausgenommen ist die Ermächtigung des BSI zur Kontrolle der Kommunikationstechnik des Bundes nach neuen §§ 4a, 4b des BSI-Gesetzes, zur Verarbeitung behördeninterner Protokollierungsdaten nach neuem § 5 des BSI-Gesetzes sowie zur Festlegung der Mindeststandards für die IT-Sicherheit der Stellen des Bundes und öffentlichen Unternehmen (§ 8 des BSI-Gesetzes).

Auch wenn die Zustimmung des Bundesrates überraschend kam, hatte doch der Bundsratsausschuss für Innere Angelegenheiten die Einberufung des Vermittlungsausschusses und Änderungen am Gesetz empfohlen, lässt gerade diese den Willen des Gesetzgebers, die IT-Sicherheit stärker in Fokus zu nehmen, eindeutig erkennen. Dabei schafft das neue Gesetz lediglich einen Rahmen für weitere Anpassungen, denn viele neue Vorschriften müssen von Verordnungen detailliert werden.

Grundsätzlich lassen sie die Neuerungen in vier große Kategorien aufteilen:

- § Erweiterung der Befugnisse des BSI
- § Schutz kritischer Infrastrukturen
- § Stärkung des Verbraucherschutzes
- § Schutz von Mobilfunknetzen

Das BSI wird durch das neue Gesetz zu einer zentralen Cybersicherheitsbehörde aufgebaut. Zum einen werden seine Kompetenzen dahingehend erweitert, dass zusätzliche Kontroll- und Prüfmechanismen etabliert werden; zum anderen bekommt das BSI die Ermächtigung, obligatorische Mindeststandards festzulegen. Das BSI wird nun im Laufe des Jahres technische Meldemöglichkeiten errichten müssen, um Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die IT-Sicherheit und der dabei beobachteten Vorgehensweisen entgegenzunehmen. Zusätzliche Kompetenzen erhält die Behörde auch in Bezug auf Telekommunikations- und Telemediendienste, sodass beim Bestehen einer konkreten akuten Gefahr bestimmte Schritte vorgenommen bzw. von bestimmten Aktionen abgesehen werden muss (§§ 7c, 7d des neuen BSI-Gesetzes).

### Was ist zu beachten?

Betreiber Kritischer Infrastrukturen sind bereits jetzt verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, und dabei den Stand der Technik einzuhalten. Diese Verpflichtung umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung.



Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Solche organisatorischen und technischen Vorkehrungen gelten dann als angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Den Betreibern kritischer Infrastrukturen sind darüber hinaus die „Unternehmen im besonderen öffentlichen Interesse“ gleichgestellt (die treffen dann die gleichen Pflichten). Dies sind solche Unternehmen, die nicht Betreiber kritischer Infrastrukturen im Sinne von BSI-Gesetz sind, dabei aber:

- > *Güter nach § 60 Abs.1 Nummer 1 und 3 der Außenwirtschaftsverordnung herstellen oder entwickeln, wie bspw. Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte,*
- > *nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind,*
- > *Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung sind oder diesen gleichgestellt sind.*

Die Unternehmen im besonderen öffentlichen Interesse werden durch die Rechtsverordnung bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind. Besonders diese Alleinstellungsmerkmale dürften für die mittelständischen IT-Unternehmen von großem Interesse sein, sind diese doch nicht selten „hidden champions“ in ihren jeweiligen Bereichen. Wie lange das BSI für die Bestimmung dieser Merkmale brauchen wird, ist noch unklar.

## Cybersicherheit & Verbraucherschutz



Darüber hinaus wird das BSI Cybersicherheitszertifikate und weitere auf die Konformität der eingesetzten Systeme gerichteten Bestimmungen treffen (müssen). Konformitätsbewertungsstellen werden dabei nur mit Erlaubnis durch das BSI tätig sein dürfen. Im Bereich des Verbraucherschutzes wird das BSI „zur Information von Verbrauchern über die IT-Sicherheit von Produkten“ ein einheitliches IT-Sicherheitskennzeichen einführen. Das IT-Sicherheitskennzeichen wird dabei jedoch keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes treffen, sodass an diese Stelle die Kluft zwischen der IT-Sicherheit und dem Datenschutz nochmals verdeutlicht wird.

## Kontakt

Sie haben Fragen zum Datenschutz?  
Wenden Sie sich gern an uns.



Olga Kunkel  
[olga.kunkel@itwirtschaft.de](mailto:olga.kunkel@itwirtschaft.de)

Kompetenzzentrum IT-Wirtschaft  
vertreten durch:

Bundesverband IT-Mittelstand e.V. (BITMi)  
Hauptstadtbüro Berlin:  
Haus der Bundespressekonferenz  
Schiffbauerdamm 40, 10117 Berlin  
T +49 30 22605 005  
[www.itwirtschaft.de](http://www.itwirtschaft.de)

## Was ist Mittelstand-Digital?

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft ist Teil der Förderinitiative Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren vor Ort helfen dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter:  
[www.mittelstand-digital.de](http://www.mittelstand-digital.de)

## Impressum

Konzeption und Text: Kompetenzzentrum IT-Wirtschaft, Olga Kunkel

Bildnachweis: Titel Unsplash / Maxim Hopman  
sowie Hirofumi Nobukuni