Deloitte.

URL: http://www.deloitte-tax-news.de/unternehmensrecht/neue-herausforderung-fuer-die-digitalisierung-deutschlands-was-das-it-sicherheitsgesetz-20-und-die-neue-kritis-verordnung-mit-sich-bringen.html

28.05.2021

Unternehmensrecht

Neue Herausforderung für die Digitalisierung Deutschlands: was das IT-Sicherheitsgesetz 2.0 und die neue KRITIS-Verordnung mit sich bringen

Erweiterter Adressatenkreis, zusätzliche Pflichten und Auswirkung auf Lieferketten – ein Überblick

Viele Unternehmen, die bisher nicht unter das BSIG fielen, müssen bald neue und strengere Anforderungen erfüllen – ohne Schonfrist. Hier werden die Neuerungen vorgestellt.

Das Inkrafttreten des IT-Sicherheitsgesetzes 2.0 ist einen Schritt näher gerückt. Mit der Beschlussfassung des Bundesrates vom 07.05.2021 stehen der Umsetzung der Änderungen an dem Bundessicherheitsgesetz (kurz „BSIG") keine wesentlichen Hürden mehr im Wege, es fehlt im Wesentlichen nur noch die Unterschrift des Bundespräsidenten. Zusätzlich hat das Bundesministerium des Innern, für Bau und Heimat (kurz „BMI") am 26.04.2021 die Konsultationsfassung der „Zweite(n) Verordnung zur Änderung der BSI-Kritisverordnung" (kurz „Zweite KRITIS-Verordnung") veröffentlicht und holte noch bis zum 17.05.2021 Stellungnahmen von betroffenen Verbänden, Fachkreisen und der Wissenschaft ein.

Erweiterung des Adressatenkreises durch IT-Sicherheitsgesetzes 2.0
Mit dem IT-Sicherheitsgesetz 2.0 wird der Sektor Entsorgung in den Kreis der möglichen Betreiber kritischer Infrastrukturen neben den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen aufgenommen.

Daneben werden nunmehr auch Unternehmen im besonderem öffentlichen Interesse vom BSIG erfasst. Diese gelten jedoch nicht als Betreiber kritischer Infrastrukturen sondern unterliegen eigenen, weiteren Pflichten (siehe sogleich). Unternehmen im besonderen öffentlichen Interesse sind beispielsweise

- Rüstungsunternehmen (§ 1 Abs. 14 Nr. 1 IT-Sicherheitsgesetz 2.0, § 60 Abs. 1 Nr. 1 und 3 Außenwirtschaftsverordnung),
- Chemieunternehmen (§ 1 Abs. 14 Nr. 3 IT-Sicherheitsgesetz 2.0, § 1 Abs. 2 Störfall-Verordnung), oder
- Größte Unternehmen Deutschlands (§ 1 Abs. 14 Nr. 2 IT-Sicherheitsgesetz 2.0).

Unklar ist noch, nach welchen wirtschaftlichen Kennzahlen die größten Unternehmen bestimmt werden. Die Kennzahlen legt das BMI in einer Rechtsverordnung fest. Nichtsdestotrotz müssen die größten, börsennotierten Unternehmen der Bundesrepublik damit rechnen, in den Adressatenkreis des IT-Sicherheitsgesetzes 2.0 zu fallen.

Zusätzliche Erweiterung des Adressatenkreises durch Zweite KRITIS-Verordnung
udem wird erwartet, dass mit der Anpassung der KRITIS-Verordnung die Anwendung des BSIG erheblich erweitert wird. Grundsätzlich gilt, dass ein Unternehmen erst dann als Betreiber einer kritischen Infrastruktur gesehen wird, wenn eine Einrichtung des Unternehmens in den Anlagen-Begriff der KRITIS-Verordnung fällt und zudem den in den Anlagen der KRITIS-Verordnung vorgesehenen Schwellenwerte erreicht. Die Zweite KRITIS-Verordnung sieht folgende Anpassungen vor:

- Als „Anlage" sollen nach § 1 Nr. 1 des Entwurfs nicht mehr nur Betriebsstätten oder Maschinen und Geräte gelten, sondern zusätzlich auch „Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind".
- Die einzelnen zahlenmäßigen Bemessungspunkte für die Anlagen sind deutlich herabgesetzt. Nunmehr erreichen wesentlich mehr Unternehmen die Schwellenwerte und gelten in Zukunft als Betreiber kritischer Infrastrukturen.

Berichten zufolge soll mit der Zweiten KRITIS-Verordnung die Anzahl der Betreiber kritischer Infrastrukturen von rund 1.600 auf ca.1870 steigen. Diese Zahl wird im Zuge einer weiteren, absehbaren Änderung noch weiter steigen, da die Zweite KRITIS-Verordnung derzeit noch

keinen Anhang für den Sektor Entsorgung enthält.

Ausweitung der Pflichten für die Unternehmen
Das IT-Sicherheitsgesetz 2.0 sieht eine Reihe von Pflichten für die Betreiber kritischer Infrastrukturen vor. Unter anderem sollen die Betreiber

- Mindestsicherheitsstandards für kritische Infrastrukturen vorsehen (z.B. der Einsatz von Intrusion Detection Systemen nach § 8a IT-Sicherheitsgesetz 2.0),
- Sicherheitsanforderungen für kritische Komponenten einhalten (siehe dazu sogleich), und
- Informationspflichten und Meldepflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (kurz „BSI") einhalten (z.B. Auflistung aller IT-Produkte, die für die Funktionalität der kritischen Infrastrukturen wichtig sind, Meldung von Störungen).

Die Unternehmen von besonderem öffentlichen Interesse sollen zudem

- sich beim BSI registrieren und einen Ansprechpartner für das BSI benennen, und
- gegenüber dem BSI mindestens alle zwei Jahren ab Verkündung des Gesetzes eine Selbsterklärung über Zertifizierungen, Sicherheitsaudits und Prüfungen sowie die Sicherung der besonders schützenswerten IT-Systeme, Komponenten und Prozesse abgeben.

Lieferkette rückt in den Fokus
Als besondere Neuerung zeigt sich die Fokussierung auf die kritischen Komponenten. Kritische Komponenten sollen IT-Produkte sein, welche

- in den kritischen Infrastrukturen eingesetzt werden,
- bedeutend für das Funktionieren des Gemeinwesens sind (da sie Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der kritischen Infrastruktur gewährleisten), und
- entweder aufgrund eines Gesetzes als kritische Komponenten bestimmt werden oder eine kritische Funktion eines Unternehmens realisieren.

Kritische Komponenten dürfen nur dann eingesetzt werden, wenn dies dem BMI vorher angezeigt wurde, eine Zertifizierung der Komponente vorliegt und der Hersteller der Komponente eine Garantieerklärung abgegeben hat. Die Garantieerklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Schließlich kann das BMI sowohl den erstmaligen als auch den weiteren Einsatz von kritischen Komponenten durch den Betreiber kritischer Infrastrukturen bei der voraussichtlichen Beeinträchtigung der öffentlichen Sicherheit und Ordnung versagen. Unter anderem soll eine Beeinträchtigung vorliegen, wenn der Hersteller z.B. von der Regierung eines Drittstaates kontrolliert wird oder, wenn er etwa die Verpflichtungen der Garantieerklärung nicht einhält.

Keine Schonfrist mehr: Die Zeit zur Umsetzung drängt
Für Unternehmen hat das Zusammenspiel von IT-Sicherheitsgesetz 2.0 und Zweiter KRITIS-Verordnung zum Teil weitreichende Konsequenzen. Während früher noch eine Übergangsfrist zur Umsetzung der neuen Anforderungen vorgesehen war, gilt nunmehr, dass Unternehmen ab dem ersten Werktag, an dem sie die Schwellenwerte der Zweiten KRITIS-Verordnung erreichen, die Anforderungen des BSIG einhalten müssen. Das heißt, ab dem ersten Tag nach Inkrafttreten des IT-Sicherheitsgesetz 2.0 und der Zweiten KRITIS-Verordnung müssen die potenziellen Betreiber kritischer Infrastrukturen die Anforderungen des IT-Sicherheitsgesetzes erfüllen. Wenn die Anforderungen nicht eingehalten werden, drohen mitunter hohe Bußgelder bis zu 20 Millionen Euro.

Unternehmen müssen daher jetzt überprüfen, ob sie in den Adressatenkreis des IT-Sicherheitsgesetz 2.0 und der Zweiten KRITIS-Verordnung fallen.
In jedem Fall sollte hierzu fachlicher Rat und erforderlichenfalls anwaltlicher Beistand gesucht werden.

Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko. Deloitte GmbH übernimmt keinerlei Garantie oder Gewährleistung noch haftet sie in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grunde empfehlen wir stets, eine persönliche Beratung einzuholen.

This client information exclusively contains general information not suitable for addressing the particular circumstances of any individual case. Its purpose is not to be used as a basis for commercial decisions or decisions of any other kind. This client information does neither constitute any advice nor any legally binding information or offer and shall not be deemed suitable for substituting personal advice under any circumstances. Should you base decisions of any kind on the contents of this client information or extracts therefrom, you act solely at your own risk. Deloitte GmbH will not assume any guarantee nor warranty and will not be liable in any other form for the content of this client information. Therefore, we always recommend to obtain personal advice.