STELLUNGNAHME

Der Mittelstand. BVMW
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschlands e.V.

Stellungnahme zum Referentenentwurf „IT-Sicherheitsgesetz 2.0“ in der Fassung vom 01.12.2020

Zentrale Forderungen des Mittelstands:

1. **BSI-Kompetenzen in gesunder Verhältnismäßigkeit ausbauen**
2. **Graduierung der Unternehmen sinnvoll gestalten**
3. **Bußgeldvorschrift transparent umsetzen**

Einleitung:

Im Zuge der fortschreitenden digitalen Transformation der deutschen Wirtschaft ist eine funktionierende Informationstechnik essentiell. Deshalb begrüßt der Bundesverband mittelständische Wirtschaft das Ziel des Entwurfes eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) des Bundesministerium des Innern, für Bau und Heimat, Informationstechnik besser zu schützen. Die Sicherheit von Informationstechnik ist Grundvoraussetzung für eine erfolgreiche digitale Transformation. Aus diesem Grund muss der vorliegende Gesetzesentwurf nicht nur unter Sicherheitsaspekten, sondern auch im Lichte der Digitalisierungseffekte auf kleine und mittelständische Unternehmen (KMU) betrachtet werden. Der Bundesverband mittelständische Wirtschaft hat bereits im Positionspapier “IT-Sicherheit im Mittelstand verankern” (05/2020) dafür plädiert, dass sich beim IT-Sicherheitsgesetz 2.0 die negativen Digitalisierungseffekte der DSGVO nicht widerholen dürfen. Im Gegenteil, stattdessen muss es das Ziel sein, Digitalisierung und damit auch IT-Sicherheit positiv in der Gesellschaft zu verankern. Dies lässt sich anhand verschiedener Faktoren, aber insbesondere mit Transparenz und Rechtssicherheit, Graduierung der Auflagen und Förderung erreichen.

Mit dem Referentenentwurf in der Fassung vom 01.12.2020, schafft das BMI nun endlich Klarheit über bisher fehlende Indikatoren und Schwellenwerte, wie der Zuordnung zu der Kategorie “Unternehmen im besonderen öffentlichen Interesse”. Der Bundesverband mittelständische Wirtschaft begrüßt, dass Unsicherheiten bezüglich der Auslegung, insbesondere für KMU, damit ausgeräumt werden.
Nichtsdestotrotz lässt der vorliegende Gesetzesentwurf an anderer Stelle die Digitalisierungseffekte weiterhin außen vor, und schafft ähnlich wie die DSGVO ein negative Wahrnehmung auf das Thema. Auch aus Perspektive der Sicherheitsaspekte geht der Gesetzesentwurf zum Teil über realistische Ziele hinaus und schafft so neue Sicherheitsrisiken. Grundsätzlich muss bemerkt werden, dass die gesamte kritische Infrastruktur im BSI gesammelt wird und damit einen “single point of failure” entwickelt. Deshalb müssen die eingereichten Sicherheitskonzepte ausreichend geschützt und klassifiziert werden.

1. BSI-Kompetenzen in gesunder Verhältnismäßigkeit ausbauen

Der Bundesverband mittelständische Wirtschaft hat in seiner digitalen Agenda des Mittelstands (03/20) bereits gefordert, dass die Zuständigkeiten im Bereich IT-Sicherheit aus Gründen der Transparenz und Effizienz stärker gebündelt und zentralisiert werden müssen. Dementsprechend ist es an einigen Stellen im Entwurf positiv zu bewerten, dass das BSI als schon bestehender zentraler Dreh- und Angelpunkt für IT-Sicherheit gestärkt wird. Besonders positiv hervorzuheben sind:

- **§ 3 Abs. 1 Warnung vor unsicheren Produkten**
- **§ 4b Allgemeine Meldestelle für die Sicherheit in der Informationstechnik**

Zu § 3 Abs. 1: Das Überprüfen und gegebenenfalls daraus resultierende Warnen vor unsicheren Produkten gehört zur zentralen Aufgabe des BSI. Es ist daher gut, dass 18 zusätzliche Stellen für diesen Zweck geschaffen werden.

Zu § 4b: Aus Gründen der Transparenz ist es wichtig, dass eine zentrale Meldestelle für die Sicherheit in der Informationstechnik geschaffen wird. Es ist aber wichtig zu betonen, dass die gemeldeten Informationen, auch wirklich nur nach den vier Nummern in Absatz 3 verarbeitet werden und es keine Verknüpfung zu § 7a und § 7b gibt. Es könnte sonst, ähnlich wie der DSGVO, das Risiko steigen, dass sich Unternehmen gegenseitig beschuldigen, IT-Sicherheitsvorgaben nicht

Stand: Dezember 2020

umgesetzt zu haben, damit das BSI Auskunftsdaten oder sich sogar "einhacken" dürfte. Dies würde zu negativen Digitalisierungseffekten in der deutschen Wirtschaft führen.

Trotz vieler Verbesserungen geht der aktuelle Gesetzesentwurf jedoch nach wie vor an mehreren Stellen zu weit, indem ausufernde und unrealistische Befugnisse für das BSI geschaffen werden. Besonders kritisch sind nach Einschätzung des Mittelstands insbesondere folgende Stellen:

- **§ 7a Untersuchung der Sicherheit der Informationstechnik**
- **§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden**
- **§ 9a Freiwilliges IT-Sicherheitskennzeichen**

zu § 7a, §7b: Es gehört zwar zu den Kernaufgaben des BSI, Bestandsdaten auszuwerten, Sicherheit der Informationstechnik zu untersuchen und Sicherheitsrisiken im Netz zu entdecken, jedoch sollte dies nur im Rahmen aller drei Paragraphen mit richterlicher Erlaubnis geschehen. Wenn ein begründeter Verdacht vorliegt, muss von einem Richter über weitere Maßnahmen entschieden werden.

- **zu § 7a: Für die Herausgabe sämtlicher Auskünfte sollten abseits von Betreibern kritischer Infrastruktur ein richterlicher Beschluss vorliegen. Die Definition auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene Produkte und Systeme ist allumfassend und zu weit. Betriebsgeheimnisse sind zu berücksichtigen. Unabhängig davon, müssen die Betreiber kritischer Infrastruktur vorrangig bei der Untersuchung der Informationstechnik behandelt werden.Der Satz " Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehene Sanktionen" ist zu streichen.**
- **zu § 7b: Unabhängig davon, ob ein richterlicher Beschluss vorliegen sollte, sollten die dargelegten Maßnahmen ausschließlich bei Betreibern von kritischer Infrastruktur durchgeführt werden**

zu § 9: Weiterhin bleibt es unrealistisch, dass das BSI sämtliche beantragten IT-Sicherheits-Produkte überprüfen kann. Wie in der Einleitung zum Gesetz beschrieben, ist IT-Sicherheit niemals statisch, das gleiche gilt dementsprechend auch für Produkte. Jedes Update kann das Sicherheitsniveau von Produkten stark verändern. Es ist außerdem fraglich, ob eine Behörde Kaufentscheidungen maßgeblich beeinflussen sollte. Dies liegt nicht im Geltungsbereich von staatlichen Institutionen, wenn auch selbstverständlich vor gefährlichen Produkten gewarnt werden sollte. Deshalb spricht sich der Mittelstand für eine reine Beschränkung auf kritische Infrastruktur aus. Vor einer Einführung des IT-Sicherheitskennzeichens müssen außerdem vorher die entsprechende Standards festgelegt sein.

2. Graduierung der Unternehmen sinnvoll gestalten

In § 2 f Absatz 14 Nummer 2 wird die neue Kategorie von Unternehmen, die sogenannten "Unternehmen im besonderen öffentlichen Interesse" eingeführt. Es ist zu begrüßen, dass der Entwurf nun Klarheit bezüglich der Graduierung und Terminologie schafft, sowie entsprechende Standards festlegt. Hierdurch werden Unklarheiten und eine hohe Bürokratielast für KMU vermieden.

3. Bußgeldvorschrift transparent umsetzen

Es ist positiv hervorzuheben, dass die Höhe der Bußgeldvorschrift im vorliegenden Entwurf weiter differenziert und eine zusätzliche Stufe für weniger schwerwiegende Verstöße eingefügt wurde. Es muss weiterhin jedoch in jedem Falle vermieden werden, dass wie bei der DSGVO durch mangelhafte Kommunikation seitens des Bundes Existenzängste bei kleinen und mittelständischen Unternehmen entstehen. Bußgelder sollten immer die letzte Sanktionsmöglichkeit sein und wirtschaftlich angemessen sein. Es ist kritisch zu hinterfragen, weshalb die Bußgeldvorschrift auch für unkritische Unternehmen gilt. Bei Verstößen gegen beispielsweise Datenschutzbestimmungen gibt es mit der DSGVO und dem BGB bereits ausreichend Sanktionierungsmöglichkeiten.

Der BVMW vertritt im Rahmen der Mittelstandsallianz über 900.000 Mitglieder. Die mehr als 300 Repräsentanten des Verbandes haben jährlich rund 800.000 direkte Unternehmerkontakte. Der BVMW organisiert mehr als 2.000 Veranstaltungen pro Jahr.

Kontakt
Bundesverband mittelständische Wirtschaft (BVMW) e. V.
Bereich Politik und Volkswirtschaft
Potsdamer Straße 7, 10785 Berlin
Telefon: + 49 30 533206-0, Telefax: +49 30 533206-50
E-Mail: politik@bvmw.de; Social Media: @BVMWeV