Wirtschaftsrat der CDU e.V.
Luisenstr. 44
10117 Berlin
Telefon: 030 / 240 87 - 227
E-Mail: b.harth@wirtschaftsrat.de

Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz) vom 02. Dezember 2020

Das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) leistet einen wichtigen Beitrag zur Erhöhung der Cybersicherheit innerhalb Deutschlands und Europas. Mit dem Gesetz nimmt Deutschland innerhalb der Europäischen Union (EU) eine führende Rolle in der Cyber- und IT-Sicherheit ein und sichert damit die langfristige digitale Transformation von Staat und Wirtschaft. Diese Führungsrolle muss dafür genutzt werden, einheitliche EU-weite Vorgaben durchzusetzen. Damit kann der europäische digitale Binnenmarkt ganzheitlich gefestigt und Unternehmen klare sowie gerechtfertigte Vorgaben gemacht werden. Gleichzeitig sind alle beteiligten Unternehmen, Anwender, Hersteller und Betreiber gefordert, aktiv zusammenzuarbeiten, um die Cyber-Resilienz der deutschen Wirtschaft zu stärken.

Die Bundesarbeitsgruppe Cyber Sicherheit im Wirtschafrat der CDU e.V. ruft dazu auf den Entwurf des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) vom 2. Dezember 2020 im weiteren Gesetzgebungsverfahren zu konkretisieren und Wettbewerbsnachteile zu beseitigen. Parallel dazu kritisiert die Bundesarbeitsgruppe das aktuelle Vorgehen des Bundesministeriums des Innern, für Bau und Heimat (BMI). Unternehmen, Länder und Verbände haben nur wenige Tage für die inhaltliche Positionierung zu dem Diskussionsentwurfs bevor der voraussichtlichen Kabinettsbefassung am 16. Dezember 2020 erhalten. Konkret fordert die Bundesarbeitsgruppe Cyber Sicherheit:

Informationsaustausch ist keine Einbahnstraße

Bereits für das erste IT-Sicherheitsgesetz hat der Wirtschaftsrat einen stärkeren Austausch von Meldungen von staatlicher Seite an Sicherheitsbehörden gefordert. In den vergangenen Jahren gab es bereits Versuche, den Informationsfluss zu erhöhen. In Einzelfällen passiert dies auch regelmäßig. Dieser Informationsfluss muss intensiviert und zu einem umfassenden, bundesweiten Lagebild ausgebaut werden.

Konkretisierung der Kategorie: Unternehmen im besonderen öffentlichen Interesse

Der Wirtschaftsrat bewertet die Einführung der Kategorie von „Unternehmen im besonderen öffentlichen Interesse“, also Unternehmen, „die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind“, als zu umfassend. Wir fordern das Bundesministerium für Wirtschaft und Energie (BMWi) und das Bundesministerium des Innern, für Bau und Heimat (BMI) dazu auf, eine Konkretisierung der Kriterien vor der

Gesetzgebung und nicht erst im Rahmen der Verordnung durchzuführen, um klarzustellen, welche Unternehmen unter §2 Abs. 14 Nr. 2 fallen.

Zusätzlich weisen wir darauf hin, dass Deutschland mit der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ einen Sonderweg im Vergleich zu anderen Mitgliedsstaaten der EU einschlägt. Das widerspricht der erwünschten Harmonisierung der nationalgeltenden Gesetze innerhalb der EU.

Bußgelder – keine Analogie zu Datenschutzverstößen

Eine Analogie zu den Bußgeldern aus der EU-Datenschutzgrundverordnung (DS-GVO) ist aus Sicht des Wirtschaftsrates nicht angemessen (§ 14 Abs. 2 BSIG). Ein Verstoß gegen Datenschutzvorschriften ohne Bußgelder führt zur Schädigung der Verbraucher, aber nicht zwingend des Unternehmens. Bei einem Verstoß gegen das IT-Sicherheitsgesetz liegt der Schaden eines Vorfalls zwingend auch beim Unternehmen. Eine versäumte Meldepflicht bei IT-Angriffen bringt keinen unternehmerischen Vorteil. Ein gehacktes Unternehmen wird hingegen schon durch die Folgen des Angriffs finanziell belastet, sodass hier eine ohnehin stärkere Eigenmotivation herrscht, entsprechend Vorkehrungen zu treffen. Zusätzliche Belastungen durch umfangreiche Bußgelder, ähnlich wie bei Verstößen gegen die DS-GVO, könnten sich kontraproduktiv auswirken und den gegenteiligen Effekt haben.

Der Wirtschaftsrat begrüßt die im Entwurf vorgeschlagenen Deckelungen der Bußgelder auf zwei Millionen Euro. Die vorgeschriebene Summe käme den Absichten des IT-SiG 2.0 nach, Unternehmen nach einem Cybersicherheits-Vorfall nicht mit überzogenen Strafen zu belasten. Jedoch fordern wir eine Streichung des Verweises auf § 30 Abs. 2 Satz 3 OWiG, da Bußgelder für juristische Personen und Personenvereinigungen weiterhin 20 Millionen Euro betragen können.

Im Übrigen begrüßt der Wirtschaftsrat, dass zumindest gegen Institutionen der sozialen Sicherung, die nicht am Wettbewerb teilnehmen, keine Bußgelder verhängt werden. Nichtsdestotrotz sollte diese Ausnahme für alle öffentlichen Stellen gelten. Das kann damit begründet werden, dass in Deutschland auch im Datenschutzrecht Bußgelder für öffentliche Institutionen

ausgeschlossen sind. Strengere Regelungen als im Datenschutzrecht können im IT-Sicherheitsrecht nicht gewollt sein und würden sich benachteiligend auswirken.

Europaweite Harmonisierung der IT-Sicherheitsgesetzgebung

Der Wirtschaftsrat begrüßt explizit, dass Deutschland – wie schon beim ersten IT-Sicherheitsgesetz – eine Pionierrolle in Europa einnimmt und somit Maßstäbe auch für zukünftige europäische Regelungen setzt. Gleichzeitig sollte verhindert werden, dass durch die gesetzlichen Vorgaben für die betroffenen Unternehmen ungleiche Rahmenbedingungen entstehen, die zu Wettbewerbsverzerrungen sowie bürokratischen Mehraufwänden führen. Die im IT-SiG 2.0 festgeschriebenen Vorgaben sollten daher europäisch skalierbar gestaltet werden. Der Wirtschaftsrat fordert, dass die Bundesregierung mit vollem Elan und schnellstmöglich an einer EU-weiten Harmonisierung auf dem Niveau des deutschen IT-Sicherheitsgesetzes arbeitet und dies im Sinne des digitalen Binnenmarktes vorantreibt.

Warnung vor Problemen mit Konformitätsbewertungsstellen

Der Wirtschaftrat kann die Bestrebungen des Gesetzgebers, das BSI als eine Konformitätsbewertungsstelle zu etablieren, nachvollziehen. Angesichts der Erfahrungen rund um die Zertifizierung von IT-Grundschutz, warnt der Wirtschaftsrat aber vor den Problemen im Kontext „Akkreditierungsstellen“. Weder erscheint eine Einordnung des BSI unter der Deutschen Akkreditierungsstelle (DAkkS) sinnvoll, noch ist der Weg einer zweiten parallel laufenden Akkreditierungsstelle durch europäisches Recht vorgesehen. Der Gesetzgeber sollte sich daher frühzeitig überlegen, ob es nicht sinnvoller wäre, die bestehenden Strukturen zu nutzen, anstatt neue zu schaffen und in direkter Konkurrenz zu stellen.

Etablierung einer Nationalen Behörde für die Cybersicherheitszertifizierung

Der Wirtschaftsrat fordert die Harmonisierung von Cybersicherheitszertifizierung innerhalb Deutschlands und Europas. Zur Erreichung dieses Ziels kann eine Nationale Behörde für die Cybersicherheitszertifizierung grundsätzlich beitragen. Diese Nationale Behörde für die Cybersicherheitszertifizierung muss es Anbietern und Herstellern von Informations- und Kommunikationstechnik (IKT) -Produkten, -Diensten und –Prozessen ermöglichen, europaweite gültige Cybersicherheitszertifizierung zu erhalten.

Generell werden von nationalen Behörden für Cybersicherheitszertifizierungen ausgestellte Zertifikate nicht von anderen Mitgliedstaaten anerkannt. Unternehmen müssen deshalb ihre IKT-Produkte, -Dienste und -Prozesse in mehreren Mitgliedstaaten zertifizieren lassen. Das ist mit hohen Kosten und großem Aufwand verbunden.

Der Wirtschaftsrat sieht es daher als kritisch, dass das BSI als nationale Konformitätsbewertungsstellen die Berechtigung dazu bekommen soll, im nationalen Alleingang für Deutschland europaweite gültige Konformitätserklärungen nach Verordnung (EU) 2019/881 für ungültig erklären zu können.

Die Aberkennung eines Zertifikats auf nationaler Ebene würde der erstrebten Harmonisierung des Binnenmarktes im Wege stehen. Wir fordern deshalb das BSI dazu auf, ein einheitliches Zertifizierungssystem zu etablieren, das kohärent und ganzheitlich ist. Das vereinfacht den Marktzugang von Unternehmen und stellt sicher, dass Produkte möglichst zeitgleich auf den europäischen Markt kommen. Zusätzlich muss das BSI seinen neugewonnen Aufgaben schnell gerecht werden. Wir fordern das Bundesamt deshalb dazu auf, zügig das notwendige Personal einzustellen.

Marktnachteile durch Sicherheitsuntersuchungen verhindern

Der Wirtschaftsrat begrüßt den in § 7a eingeschlagenen Weg zur Untersuchung der Sicherheit der Informationstechnik. Dies kann aber nur gelingen, wenn ein Weg aufgezeigt wird, der wirklich allen Marktteilnehmenden die gleichen Bedingungen bietet. Eine komplette Abdeckung des Marktes ist zwingend erforderlich. Keinesfalls darf es dazu führen, dass zum Beispiel kleine, deutsche Startups Marktnachteile erfahren, weil sie nicht zeitnah die gleichen Sicherheitsnachweise durch das BSI erhalten wie etablierte Anbieter. Es drohen außerdem Engpässe bei den Sicherheitsuntersuchungen von Systemen, wenn das BSI alleine dafür zuständig sein wird. Daher muss bereits jetzt über weitere Möglichkeiten der Prüfung nachgedacht werden und eine externe, zertifizierte Prüfung durch Dienstleister möglich gemacht werden.

Konkretisierung beim Verbot des Einsatzes von Produkten

Der Wirtschaftsrat fordert eine Konkretisierung des Vorgehens, wenn der Einsatz von bestimmten Produkten oder Komponenten untersagt wird, die sich bereits im Einsatz befinden. Zentrale Fragen müssen in diesem Zusammenhang dringend beantwortet werden:

- Müssen die Produkte nachträglich entfernt bzw. ausgetauscht werden?
- In welchem Zeitraum wäre der Austausch durchzuführen?
- Wird es Ausnahmetatbestände geben, zum Beispiel wenn der Tausch eines Produktes zwangsläufig zu Architekturänderungen führen würde?
- Wird es die Möglichkeit geben, den Austausch durch zusätzliche risikomitigierende Maßnahmen zu vermeiden?
- Wer trägt bei einer solchen Entscheidung die Kosten für den Umbau?

Die letzten Jahre haben weltpolitisch leider gezeigt, dass alte, als unverbrüchlich geltende staatliche Beziehungen ihren Wert verlieren und auch heute bereits Produktauswahlen in zunehmendem Maße international politisch beeinflusst werden. Betreiber brauchen daher die Investitionssicherheit und die Garantie, nicht indirekt zum politischen Spielball zu werden.

Harmonisierung internationaler Cybersicherheits-Standards und Berücksichtigung des existierenden Normenwerks

Die Notwendigkeit einheitlicher Standards sollte nach Möglichkeit nicht nur europäisch, sondern global betrachtet werden. Ein Beispiel ist die gegenseitige Anerkennung der Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik und der NIST (NIST 800-53). Die weltweite Einhaltung von Cyber- und IT-Sicherheit-Standards kann nur durch eine starke Ausrichtung des europäischen Binnenmarktes und der Zusammenarbeit aller EU-Mitgliedstaaten gelingen. Alleingänge von einzelnen EU-Staaten würden nur dazu führen den vorhandenen, rechtlichen Flickenteppich weiterzuspinnen und den Kosten-, Zeit- und Effizienz-Aufwand für alle relevanten Beteiligten sowie die Wettbewerbsverzerrungen zu erhöhen. Parallel dazu würden weitere Vorgaben zu zusätzlichen Unsicherheiten bei Unternehmen und Verbrauchern führen.

Sollte keine gegenseitige Anerkennung möglich sein, wären Hinweise darauf, in welchen Bereichen ein unterschiedliches Verständnis (seitens BSI) hinsichtlich der Informationssicherheit und deren korrespondierenden Maßnahmen bestehen, hilfreich. So wären die Anforderungen an die Informationssicherheit von Produkten für den globalen Markt gut aufzusetzen.

Parallelsysteme vermeiden: Stand der Technik sollte das BSI nicht allein vorgegeben

Der aktuelle Entwurf zum IT-SiG 2.0 sieht vor, Kompetenzen, die bisher der Normung zugehörig sind, zunehmend beim BSI zu zentralisieren und damit ein teilweise paralleles System aufzubauen. Nach Abschnitt 13.b. § 8a Abs. 1b müssen Betreiber kritischer Infrastrukturen, Angriffssysteme nach dem Stand der Technik einsetzen, welche vom BSI durch eine technische Richtlinie vorgegebenen wird.

Hierbei handelt es sich um einen unnötigen Eingriff in den Markt, der zu Wettbewerbsverzerrungen führt und Innovationen hemmt. Etablierte Sicherheitslösungen, welche die spezifischen Anforderungen der Betreiber erfüllen, müssten dann ggf. aufwendig ausgetauscht werden, ohne einen Zugewinn an Sicherheit zu erzielen. Noch weniger kann das BSI allgemein den Stand der Technik von IT-Sicherheitslösungen definieren, wie in 2.h. § 3 Abs. 20 gefordert. Hier ist der Markt gefragt und die Betreiber der kritischen Infrastrukturen sind zu beteiligen.

Eine detaillierte Registrierung aller IT-Komponenten beim BSI ist nicht sinnvoll

Der Wirtschaftsrat begrüßt, dass von der Übermittlung einer Liste aller IT-Produkte, die für die Funktionsfähigkeit der kritischen Infrastruktur notwendig sind (Abschnitt13.c. § 8a Abs. 3), abgesehen wird. Die Registrierung hätte einen erheblichen zusätzlichen Verwaltungsaufwand zur Folge. Darüber hinaus hätte eine solche Auflistung unter Umständen ein mögliches Einfallstor für Angreifer sein können, falls unbefugte Dritte Zugang zu diesen Listen erhalten hätten.

Untersuchung der Sicherheit in der Informationstechnik

Laut § 7a BSIG-E in Verbindung mit §§ 7, 7a, 7b und 7c BSIG-E kann das BSI einen Hersteller dazu auffordern, Auskünfte über technischen Details eines Gerätes oder Systems zu geben. Konkretisiert wird aber nicht, unter welchen Befugnissen das BSI diese Informationen einfordern darf, noch welche Beschränkungen für das Bundesamt gelten. Weiterführend hat das

Bundesamt auch die Befugnis, Information zu Schwachstellen an andere Sicherheitsbehörden weiterzuleiten. Wir sehen dies als kritisch. Es muss einen transparenten Prozess darüber geben, unter welchen Befugnissen das BSI arbeitet und welche Informationen an andere Sicherheitsbehörden weitergegeben werden.