TÜV VERBAND

Stellungnahme
zum geplanten IT-Sicherheitsgesetz 2.0

Berlin
7. Dezember 2020

Stellungnahme zum IT-SiG 2.0

Kommentierung des Referentenentwurfes vom 01.12.2020 zum Entwurf eines zweiten IT-Sicherheitsgesetzes (IT-SiG 2.0)

Arvin Keynes via Unspalsh

Stellungnahme zum IT-SiG 2.0

Kommentierung des Referentenentwurfes vom 01.12.2020 zum Entwurf eines zweiten IT-Sicherheitsgesetzes (IT-SiG 2.0)

Am 2. Dezember 2020 hat das Bundesministerium des Innern, für Bau und Heimat (BMI) eine Version des Referentenentwurfes vom 1. Dezember 2020 zum zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) auf seiner Webseite als „Diskussionsentwurf" veröffentlicht. Stellungnahmen dazu können demnach bis zum 9. Dezember 2020 eingereicht werden. Dabei wird auf den noch laufenden Prozess der Ressortabstimmung verwiesen, durch welchen noch „materielle Veränderungen am Diskussions-entwurf (auch in nicht aufgeführten Bestimmungen)" zu erwarten seien.

Der TÜV-Verband hält die sehr kurze Frist von fünf vollen Werktagen zur Stellungnahme, zu einem noch nicht durch die Ressorts abgestimmten Diskussionsentwurf, für inakzeptabel. Das IT-Sicherheitsgesetz 2.0 ist das zentrale Legislativvorhaben in dieser Legislatur zur Weiterentwicklung des nationalen Regulierungsrahmens im Bereich Cybersicherheit. Eine umfangreiche sowie tiefgreifende und der Bedeutung des Themas angemessene Befassung durch die Verbände und ihrer Unternehmen ist in solch einer kurzen Frist in keiner Weise möglich.

Grundsätzlich hätte es zuerst einer Einigung der Ressorts bedurft und daran anschließend einer mindestens vierwöchigen Verbändeanhörung.

Der TÜV-Verband begrüßt die mit dem Gesetzesentwurf verbundene Zielsetzung, der zunehmenden Bedrohungslage für informationstechnische Systeme in verstärktem Maße Rechnung zu tragen. Die Erfahrungswerte seit der Einführung des IT-Sicherheitsgesetzes vom 17. Juli 2015 zeigen bereits, dass gesetzliche Regulierung grundsätzlich geeignet ist, um die Resilienz der Wirtschaft und der Verbraucher:innen gegenüber den weiterhin zunehmenden Gefahren aus dem Cyberraum zu erhöhen.

Die hier verfolgte Lösung, den Ordnungsrahmen durch das zweite IT-Sicherheitsgesetz zu erweitern, wird unterstützt. Hierdurch nimmt der Staat seine Schutzfunktion für die Bürger:innen und zum Schutz der öffentlichen Informationstechnik sowie für eine resiliente Wirtschaft wahr. Mit dem vorliegenden Referentenentwurf legt die Bundesregierung ein umfangreiches Regelungswerk vor, welche das Thema der IT-Sicherheit aus unterschiedlichen Perspektiven adressiert.

Kernforderungen

1. **Sicherheit im Cyberraum durch eine höhere Resilienz stärken**
   Der TÜV-Verband begrüßt das mit dem IT-SiG 2.0 verbundene Ziel, mehr Sicherheit im Cyberraum zu schaffen und die Widerstandsfähigkeit der kritischen Infrastrukturen in Deutschland zu erhöhen. Die Ausweitung der KRITIS-Sektoren sowie die Adressierung von „Unternehmen im besonderen öffentlichen Interesse" erscheint vor dem Hintergrund der weiterhin zunehmenden Cyberrisiken als adäquates Mittel. Zu begrüßen ist auch die Einbeziehung entsprechender „kritischer Komponenten".

2. **IT-Sicherheitskennzeichen konkretisieren und Transparenz im Markt herstellen**
   Zur Vertrauensbildung beim Verbraucher ist es bei der Ausgestaltung des IT-Sicherheitskennzeichens zentral, dessen Aussage so konkret wie möglich darzustellen und damit Fehlinterpretationen der Verbraucher:innen vorzubeugen. Der TÜV-Verband ist der Überzeugung, dass nur die gemeinsame Betrachtung der Schutzziele Safety, Security und Privacy einem umfassenden Sicherheitsversprechen dauerhaft gerecht werden kann. Ebenfalls rät der TÜV-Verband von der Verwendung eines hoheitlichen Symbols als Bestandteil des Prüfzeichen ab.

3. **Ordnungspolitische Grundsätze wahren**
   Sowohl die Übertragung neuer Aufgaben an das BSI als auch die Personalpolitik des BSI sollten dem Grundsatz des Subsidiaritätsprinzips entsprechen und sich gleichfalls an den Grundsätzen der Staatsentlastung orientieren. Dem folgend sollen sich Staat und Behörden auf ihre originären und hoheitlichen Aufgaben konzentrieren können, die nicht anderweitig durch nicht-staatliche Akteure ebenso effizient erfüllt werden können. Die TÜV-Unternehmen haben ihrerseits massiv in Kompetenzaufbau investiert und sehen sich in der Lage, ihre Rolle in diesem System im Rahmen der Konformitätsbewertung wahrzunehmen.

4. **BSI als Cybersicherheitsbehörde auf hoheitliche Aufgaben konzentrieren**
   Durch die dem BSI zugedachten Tätigkeiten in der Akkreditierung, der Zertifizierung, der Marktaufsicht und der Regelsetzung wird das BSI politisch angreifbar, denn es drohen Interessenkonflikte und eine Aufgabenüberfrachtung. Durch die gleichzeitige Ausübung von Rollen, die im Sinne eines Systems basierend auf Check-and-Balances austariert und getrennt sein sollten, wird es der Behörde systematisch erschwert, Vertrauen zu schaffen und die Unabhängigkeit und Neutralität sicherzustellen, die es dazu bedarf.

5. **Detektion von Sicherheitsrisiken als Pflicht der jeweiligen Betreiber verankern**
   Zur Detektion von Sicherheitsrisiken in digitalen Infrastrukturen sollte das BSI vom Gesetzgeber ausschließlich für die Infrastrukturen des Bundes beauftragt werden. Unternehmen im Bereich der kritischen Infrastrukturen, der digitalen Dienste und Unternehmen im öffentlichen Interesse sollten stattdessen verpflichtet werden, gegenüber dem BSI regelmäßig den Nachweis zu erbringen, dass mögliche Sicherheitsrisiken durch qualifizierte unabhängige Dritte detektiert wurden.

Ordnungspolitische Grundsätze

Das Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird im vorliegenden Entwurf mit einer Vielzahl neuer Aufgaben und entsprechend auch mit mehr Ressourcen ausgestattet. Dem beachtlichen Erfüllungsaufwand, der mit dem zweiten IT-Sicherheitsgesetz einhergeht, steht eine zu erwartende Personalaufstockung des BSI um 799 Planstellen und mit Personalkosten in Höhe von jährlich rund 56,9 Millionen Euro (vgl. E3) gegenüber. Mit Blick auf qualifizierte IT-Sicherheitsexperten sollte sowohl die Übertragung neuer Aufgaben an das BSI als auch die Personalpolitik des BSI, angesichts der ohnehin angespannten Finanz- und Arbeitsmarktsituation, dem Grundsatz des Subsidaritätsprinzips entsprechen. Weiterhin empfiehlt der TÜV-Verband, sich am Grundsatz der Staatsentlastung zu orientieren. Dem folgend sollen sich Staat und Behörden auf ihre originären und hoheitlichen Aufgaben konzentrieren können, die nicht anderweitig durch nichtstaatliche Akteure ebenso wirksam erfüllt werden können.

Die dem BSI zugedachte Aufgabenkonzentration und Aufgabenfülle sieht der TÜV-Verband, dies insbesondere unter dem Aspekt der Neutralität und Unabhängigkeit, aus ordnungspolitischen Grundsätzen heraus mit Sorge. Durch die ihm zugedachten Tätigkeiten in der Akkreditierung, der Zertifizierung, der Marktaufsicht und der Regelsetzung wird das BSI politisch angreifbar. Durch die gleichzeitige Ausübung von Rollen, die im Sinne eines Systems basierend auf Check-and-Balances austariert und getrennt sein sollten, wird es der Behörde systematisch schwergemacht, Vertrauen zu schaffen und die Unabhängigkeit und Neutralität sicherzustellen, die es dazu bedarf.

Zum Schutz seiner Unabhängigkeit und zur Vermeidung von Interessenkonflikten, sowie damit verbundenen Beeinträchtigungen des Qualitäts- und Sicherheitsniveaus, sollten Prüforganisationen sowie Genehmigungs- und Aufsichtsbehörden jeweils nur eine Rolle wahrnehmen. Das heißt, dass Genehmigungs- und Aufsichtsbehörden sowie akkreditierende und notifizierende Stellen nicht als Zertifizierungsstellen fungieren sollten. Aufgrund ihrer Funktion als notifizierende Behörde sollte sie somit weder Konformitätsbewertungen noch Beratungsleistungen auf wettbewerblicher Basis anbieten. Dies dient dem konsequenten Ausschluss von Interessenskonflikten. Die TÜV-Unternehmen haben ihrerseits massiv in Kompetenzaufbau investiert und sehen sich in der Lage, eine wichtige Rolle in diesem System im Rahmen der Konformitäts-bewertung wahrzunehmen.

Eine klare Aufgabenabgrenzung stärkt das notwendige Vertrauen in das Gesamtsystem und sorgt für faire, klare und transparente Wettbewerbsbedingungen sowie ein einheitliches Level-Playing-Field in Deutschland und Europa.

Kritische Infrastrukturen absichern (Artikel 1, §2)

Der TÜV-Verband begrüßt ausdrücklich das hier konkretisierte Ansinnen, die Resilienz von kritischen Infrastrukturen zu erhöhen. Die Ausweitung der KRITIS-Sektoren sowie die Adressierung von „Unternehmen im besonderen öffentlichen Interesse", an die weitere Vorgaben zur Erfüllung definierter Sicherheitsanforderungen geknüpft sind, erscheint vor dem Hintergrund der weiterhin zunehmen Cyberrisiken als adäquates Mittel. Zu begrüßen ist auch die Einbeziehung entsprechender „kritischer Komponenten", die den technologischen Kern bilden und damit das Rückgrat der digitalen Infrastruktur Deutschlands bilden.

Freiwilliges IT-Sicherheitskennzeichen (§9c)

Wesentliche Aspekte des IT-Sicherheitskennzeichens, wie zum Beispiel Einzelheiten zu dessen grafischer Gestaltung, dessen Inhalt oder dessen Verwendung, sollen dem vorliegenden Entwurf folgend, im Nachgang nach Anhörung der Wirtschaftsverbände mittels Rechtsakt gesondert bestimmt werden (siehe §10, Absatz 3). Da diese Details essentiell für eine konkrete Bewertung sind, kann der TÜV-Verband zum jetzigen Zeitpunkt nur im Allgemeinen dazu Stellung beziehen, bietet jedoch seine Expertise und Unterstützung zu Fragen der weiteren inhaltlichen Ausgestaltung des IT-Sicherheitskennzeichens an.

Das vom Gesetzgeber verfolgte Ziel, dem Verbraucher durch ein IT-Sicherheitskennzeichen eine verlässliche Orientierung über die Einhaltung der anzuwendenden IT-Sicherheitsanforderungen an das Produkt, beziehungsweise den Hersteller und damit eine fundierte Kaufentscheidung zu ermöglichen, ist grundsätzlich begrüßenswert. Den hier gewählten nationalen Regulierungsansatz für das IT-Sicherheitskennzeichen gilt es, in Hinblick auf das europäische Gesetz zur Cybersicherheitszertifizierung (Cybersecurity Act, CSA) und deren zu erwartenden Schemes, wie sie im Union Rolling Work Programm der ENISA zu erwarten sind, zu prüfen. Ansonsten besteht die Gefahr, dass aufgrund unterschiedlicher regulatorischer Ansätze zur Cybersicherheitszertifizierung, auf nationaler und europäischer Ebene, nicht mehr, sondern weniger Orientierung für den Verbraucher geschaffen wird. Der CSA hat hierfür europaweit die notwendigen regulativen und organisatorischen Rahmenbedingungen geschaffen, die es jetzt zu nutzen gilt.

Der TÜV-Verband erachtet es für die Wirksamkeit des IT-Sicherheitskennzeichens zur Vertrauensbildung beim Verbraucher als zentral, den Aussagegehalt des geplanten IT-Sicherheitskennzeichens so konkret wie möglich darzustellen und damit möglichen Fehlinterpretationen des Verbrauchers vorzubeugen. Das gilt auch vor dem Hintergrund, dass das im Rahmen des IT-Sicherheitskennzeichens zum Ausdruck gebrachte Sicherheitsversprechen eben nicht vollumfassend, sondern ausschließlich auf den Teilaspekt der Cybersecurity begrenzt ist. Der TÜV-Verband ist der Überzeugung, dass nur die gemeinsame

Betrachtung der Schutzziele Safety, Security und Privacy einem notwendig umfassenden Sicherheitsversprechen dauerhaft gerecht werden kann.

Ebenfalls rät der TÜV-Verband von der Verwendung eines hoheitlichen Symbols als Prüfzeichen ab. In den ersten bekannt gewordenen grafischen Entwürfen wurde der Bundesadler als Teil des Prüfzeichens sichtbar. Die Verwendung dessen suggeriert dem Verbraucher jedoch eine geprüfte Sicherheit durch den Staat – was faktisch nur im Rahmen der Marktüberwachung, also fallweise und in geringen Fallzahlen – der Fall wäre. Eine Plausibilitätsprüfung durch eine Behörde sollte nicht zur Verwendung des Bundesadlers führen.

Eine "Plausibilitätsprüfung" der eingereichten Dokumente zur Vergabe das IT-Sicherheitskennzeichens hält der TÜV-Verband für unzureichend. Auch hier ist es im Sinne der Transparenz zur Steuerung der Verbrauchererwartung wichtig herauszustellen, dass ein solcher Prozess nicht vergleichbar mit einer umfassenden und tiefer fundierten Prüfung ist, wie sie als Grundlage für eine Zertifizierung üblich ist. Ein Prüfzeichen, welches Vertrauen und Sicherheit schaffen soll, darf nach Überzeugung des TÜV-Verbands nur auf Basis einer unabhängigen Zertifizierung erfolgen.

BSI als nationale Behörde für die Cybersicherheitszertifizierung (§9a)

Dem vorliegenden Entwurf nach wird das BSI als nationale Behörde für Cybersicherheitszertifizierung ausgestattet, was auch im Einklang mit der Regelung des europäischen Cybersecurity Acts steht (Art. 58).

Dadurch wird das BSI in die Rolle versetzt, auch den Konformitätsbewertungsstellen die Befugnis zu erteilen, für Cybersicherheitszertifizierungen tätig zu werden. Der TÜV-Verband sieht die Notwendigkeit, hier auch Kohärenz zur Regelung des CSA Art. 60 (1) sicherzustellen. Dies gilt insbesondere mit Blick auf die Rolle der DAkkS.

Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden (§7b)

Der TÜV-Verband regt an, die auf die in §7b beschriebene Art und Weise gewonnenen Informationen an einen konkreten Zweck zu binden, etwa zur Erstellung eines entsprechenden Lagebilds. Aus dem vorliegenden Referentenentwurf geht weiterhin nicht hervor, welche technischen Maßnahmen konkret vom BSI zur Detektion von Sicherheitsrisiken genutzt werden dürfen. Die Konkretisierung der möglichen technischen Maßnahmen erscheint auch aufgrund der Tatsache geboten, dass die hier implizierten

Szenarien weit über das, was ein reiner Portscan, der hier als einziges technisches Mittel genannt wird, leisten kann, hinausgehen. Offene Ports dürfen dabei nicht per-se einem Risiko zugerechnet werden, sondern sind in der Erbringung technischer Dienste absolut notwendig. Ob und in welchem Umfang Tools auch zur Dienst- und Versionserkennung von Systemen eingesetzt werden dürfen bleibt ebenfalls unklar. Aus Sicht des TÜV-Verbands ist der Portscan hier des Weiteren nicht ausreichend vom Einsatz eines Schwachstellen-Scanners abgegrenzt bzw. dessen Nutzung im vorliegenden Entwurf des Legislativvorhabens nicht hinreichend geregelt.

Der TÜV-Verband empfiehlt weiterhin, das BSI-Mandat zur „aktiven" Sicherheitsanalyse hier auf Infrastrukturen des Bundes zu begrenzen. Um das gewonnene Vertrauen auch gegenüber den Unternehmen nicht zu gefährden, sollte das BSI zur Detektion von Sicherheitsrisiken in digitalen Infrastrukturen vom Gesetzgeber ausschließlich mit einer eindeutig defensiven Arbeitsweise beauftragt werden.

Unternehmen im Bereich der kritischen Infrastrukturen, der digitalen Dienste und Unternehmen im öffentlichen Interesse sollten im Sinne einer höheren Resilienz stattdessen verpflichtet werden, gegenüber dem BSI regelmäßig den Nachweis zu erbringen, dass mögliche Sicherheitsrisiken ihrer öffentlich zugänglichen Infrastruktur durch qualifizierte unabhängige Dritte im Rahmen regelmäßiger „Spotchecks" detektiert wurden. Die Pflicht zur Durchführung dieser Sicherheitsanalysen sollte jedoch bei den Betreibern der jeweiligen Infrastrukturen selbst verankert werden.

Autor und Ansprechpartner

Marc Fliehe
Bereichsleitung Digitalisierung & IT-Sicherheit
E-Mail: marc.fliehe@vdtuev.de
Tel. +49 30 760095 460
www.vdtuev.de

Der Verband der TÜV e. V. vertritt die politischen und fachlichen Interessen seiner Mitglieder gegenüber Politik, Verwaltung, Wirtschaft und Öffentlichkeit. Der Verband setzt sich für technische und digitale Sicherheit bei Produkten, Anlagen und Dienstleistungen durch unabhängige Prüfungen und qualifizierte Weiterbildung ein. Mit seinen Mitgliedern verfolgt der TÜV-Verband das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und Vertrauen für die digitale Welt zu schaffen.

Herausgeber
Verband der TÜV e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@vdtuev.de
www.vdtuev.de