Positionspapier zum IT-Sicherheitsgesetz 2.0

Das geplante IT-Sicherheitskennzeichen muss auf internationalen und Europäischen Normen und Standards basieren.

Dezember 2020

- Keine Parallelstrukturen aufbauen: Unsere Qualitätsinfrastruktur ist effizient und Grundlage für wirtschaftlichen Erfolg.
- Europäisch und international denken: Der Weg zu europäischen und internationalen Standards und Märkten führt über DIN und DKE.
- Standortvorteil nutzen: DIN und DKE sind Marktführer für IT-Sicherheits-Standardisierung.

DIN e. V.

Saatwinkler Damm 42/43
13627 Berlin
www.din.de

Kontakt:

Katja Krüger
Senior Government Relations Manager
Tel.: 030 2601-2439
E-Mail: katja.krueger@din.de

DKE

Stresemannallee 15
60596 Frankfurt
Germany
www.dke.de

Kontakt:

Johannes Koch
Leiter Nat. Normungspolitik
Tel.: 069 6308-268
E-Mail: johannes.koch@vde.com

Sichere und geschützte IT-Systeme sind zu einem wesentlichen Erfolgsfaktor der Digitalwirtschaft geworden. Wenn im Rahmen der digitalen Transformation immer mehr Internet of Things (IoT)-fähige Geräte in Unternehmen und Privathaushalten Einzug halten, rücken auch Fragen nach Produktsicherheit und -qualität sowie Verbraucherschutz vermehrt in den Fokus. DIN und DKE begrüßen vor diesem Hintergrund den Ansatz des geplanten IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) zur Stärkung der IT-Sicherheit in Deutschland. Mit dem darin vorgesehenen freiwilligen IT-Sicherheitskennzeichen sollen Risikobewusstsein und Beurteilungsfähigkeit von Verbrauchern gefördert werden. DIN und DKE, die nationalen Normungsorganisationen, kritisieren allerdings die in der Umsetzung des Kennzeichens vorgesehene Prozess- und Kompetenzverteilung nachdrücklich. Ein paralleles System zur Erarbeitung des Standes der Technik, einschließlich Konformitätsbewertung und Zertifizierung kann nicht im Interesse der staatlichen Regelsetzung sein, da es zu einer Zersplitterung der IT-Sicherheitsmarktes führen kann. Der Gesetzgeber sollte daher unbedingt auf bewährte Strukturen und die öffentlich-private Partnerschaft mit der deutschen Normung und weiteren Institutionen der nationalen Qualitätsinfrastruktur zurückgreifen.

Eine funktionierende Qualitätsinfrastruktur ist Grundlage für wirtschaftlichen Erfolg.

In Deutschland und Europa arbeiten Normung, Messwesen, Prüfdienstleister, Akkreditierung und Zertifizierung im Rahmen einer konsistenten Qualitätsinfrastruktur Hand in Hand, um die Sicherheit von Produkten und den Schutz von Verbrauchern sicherzustellen. Dieses System mit seinen spezifischen Zuständigkeiten hat sich seit Jahrzehnten bewährt.

- Eine effiziente Qualitätsinfrastruktur stellt die Einhaltung hoher Anforderungen an die Sicherheit und Qualität von Produkten und Dienstleistungen sicher.
- Der aktuelle Referentenentwurf zum IT-SiG 2.0 sieht vor, Kompetenzen, die bisher der Normung zugehörig sind, zunehmend beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu zentralisieren und damit ein paralleles System zur nationalen Qualitätsinfrastruktur aufzubauen[1]. Ein solches Parallelsystem zur Erstellung von technischen Richtlinien, Prüfverfahren und Konformitätsbewertungsprogrammen schafft unnötige Bürokratie, doppelte und längere Verfahren, zusätzliche Kosten und verschenkt das Potenzial für Synergien.
- Bei der Umsetzung des freiwilligen IT-Sicherheitskennzeichens sollte unbedingt auf die bewährten Prozesse der nationalen Qualitätsinfrastruktur zurückgegriffen werden, indem dem Kennzeichen insbesondere Europäische und internationale Normen und Standards zugrunde gelegt werden.

[1] z. B. in § 8a Abs. 1a BSIG-E: Demnach wird die Einhaltung des Stands der Technik für die Betreiber von Kritischen Infrastrukturen dann vermutet, wenn die getroffenen Maßnahmen einer Technischen Richtlinie (TR) des BSI in der jeweils geltenden Fassung entsprechen. Dies ist nicht nur im Hinblick auf das paritätisch ausgestaltete, nationale Normungsverfahren problematisch, sondern auch für die Schaffung von international und allgemein anerkannten Normen und Standards durch die Normenorganisationen ISO/IEC und CEN/CENELEC.

Durch kohärente internationale Normen haben deutsche Unternehmen Zugang zu Weltmärkten und gestalten diese mit. Der Weg zu europäischen und internationalen Standards führt über DIN und DKE.

Mit dem Normenvertrag von 1975 hat die Bundesrepublik Deutschland DIN als nationale Normungsorganisation und Vertreter Deutschlands in der europäischen und internationalen Normung anerkannt. Die Deutsche Normungsstrategie (2016) bekräftigt den Auftrag an DIN und DKE, als führende Moderationsplattformen Normungs- und Standardisierungsprozesse über die Grenzen der jeweils eigenen Organisation hinweg, auch für Foren und Konsortien, zu koordinieren. Gleichzeitig wird sichergestellt, dass das deutsche Normenwerk, bestehend aus internationalen, Europäischen und nationalen Normen, in sich kohärent und widerspruchsfrei ist. Die deutsche Wirtschaft baut auf dieses einheitliche Normenwerk, das ihr den Zugang zu Weltmärkten deutlich und nachhaltig erleichtert.

- Nationale technische Richtlinien, die außerhalb des bestehenden Normungs- und Standardisierungssystems erstellt werden, schaffen zusätzlichen Orientierungs- und Erfüllungsaufwand für Hersteller, Anwender und Verbraucher, führen zu höheren Kosten, begünstigen den Aufbau nicht-tarifärer Handelshemmnisse und wirken sich nachteilig auf die heimische Wirtschaft aus, da ihre Inhalte konträr zu europäischen und internationalen Normen und Standards sein können Die dadurch entstehenden Barrieren wirken einer europäischen Harmonisierung bei der Entwicklung von IT-Sicherheitsstandards im gemeinsamen europäischen Binnenmarkt entgegen.
- DIN und DKE bieten dem BSI zur Formulierung technischer Richtlinien den engen Schulterschluss an, um soweit möglich internationale bzw. europäische Lösungen anzustreben. Über DIN und DKE können Mitarbeiter des BSI die Erarbeitung kohärenter Normen und Standards anstoßen und in europäischen und internationalen Standardisierungsgremien mitwirken.

Marktführerschaft in der Standardisierung für IT-Sicherheit.

Im Bereich IT-Sicherheit hält Deutschland über DIN und DKE mit der Führung zentraler europäischer[2] und internationaler[3] Arbeitsgremien die Marktführerschaft in der IT-Sicherheits-Standardisierung – ein Standortvorteil, den es zu nutzen gilt. In diesen Gremien werden grundlegende Normen zur IT-Sicherheit gepflegt, beispielsweise die *DIN EN ISO/IEC 27000-Normenreihe für „Informationssicherheit-Managementsysteme“*, die *ISO/IEC 15408 „Evaluationskriterien für IT-Sicherheit"* oder die *Normenreihe IEC 62443 „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“.* Diese internationalen Normen werden von deutschen Unternehmen erfolgreich angewendet. Die Konsolidierung der nationalen Meinung erfolgt im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) und im DKE-Normungskomitee „IT-Sicherheit in der Automatisierungstechnik“.

- Die konstruktive Zusammenarbeit zwischen BSI, Wirtschaft, Wissenschaft und Forschung in bestehenden und künftigen Normungsgremien sollte fortgesetzt und ausgebaut werden.

[2] CEN/CENELEC JTC 13 „Cybersecurity and Data Protection“
[3] ISO/IEC JTC1/SC 27 „Information Security, Cybersecurity and Privacy Protection“; IEC/TC 65/WG 10 “Security for industrial process measurement and control - Network and system security”

- Ein Beispiel, wie dies gelingen kann, ist die Erarbeitung der *DIN SPEC 27072 „IoT-fähige Geräte - Mindestanforderungen zur Informationssicherheit“*[4]. Der Standard richtet sich vor allem an Hersteller, Entwickler und Beschaffer entsprechender Produkte und kann als Grundlage zur Ausgestaltung des geplanten IT-Sicherheitskennzeichens genutzt werden.
- Ein weiteres Beispiel ist der Branchenspezifische Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr (DIN VDE V 0832-700), der durch das BSI anerkannt wurde.
- Über DIN und DKE besteht die Möglichkeit, diese und ähnliche Inhalte in die europäische und internationale Normung einzubringen.

Ziel des IT-Sicherheitsgesetzes 2.0 ist ein ausreichendes Schutz- und Sicherheitsniveau, insbesondere für Verbraucher. Dieses Ziel kann aus den dargelegten Gründen bestmöglich erreicht werden, wenn dem einzuführenden IT-Sicherheitskennzeichen internationale und Europäische Normen zugrunde gelegt werden, an deren Erarbeitung und Pflege sich deutsche Stakeholder sowie die öffentliche Hand, z. B. vertreten durch das BSI, über die nationalen Normungsorganisationen DIN und DKE aktiv beteiligen. Ergänzt werden können diese Normen durch Standards, die mit dem deutschen Normenwerk kohärent sind (z. B. DIN SPEC 27072). Dadurch beugt der Gesetzgeber einer Fragmentierung der Standardisierungslandschaft und der digitalen Märkte vor, schafft praxistaugliche Regeln für Hersteller, Anwender, Beschaffer und Verbraucher und stellt sicher, dass die geschaffenen Lösungen europäisch skalierbar sind.

Wir empfehlen daher folgende inhaltliche Ergänzungen zum Diskussionsentwurf des Bundesministeriums des Innern, für Bau und Heimat vom 01.12.2020:

- Zu § 3 Abs. 1 Satz 2 Nr. 20 BSIG-E (S. 6 im Referentenentwurf): „Weiterentwicklung des Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung von bestehenden, insbesondere internationalen und europäischen, Normen und Standards.“
- Zu § 9c Abs. 3 Nr. 3 BSIG-E (S. 22 im Referentenentwurf): „Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus vom Bundesamt für die Anwendung als geeignet befundenen internationalen, europäischen und nationalen Normen und Standards, die den Stand der Technik abbilden. Liegt für einen Anwendungsbereich keine solche Norm oder kein solcher Standard vor kann das Bundesamt ein solches Projekt bei den nationalen Normungsorganisationen initiieren oder eine Technische Richtlinie erarbeiten, die den jeweiligen Anwendungsbereich umfasst und soweit möglich auf bestehende Normen oder Teile davon verweist. Wird ein Anwendungsbereich von mehr als einer Technischen Richtlinie umfasst, richten sich die Anforderungen nach der jeweils spezielleren Technischen Richtlinie. Liegt für die jeweilige Produktkategorie keine Technische Richtlinie vor, ergeben sich die IT-Sicherheitsanforderungen aus branchenabgestimmten IT-Sicherheitsvorgaben, sofern das Bundesamt festgestellt hat, dass diese Vorgaben geeignet sind, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese

[4] Das Dokument wurde unter Beteiligung des BSI erarbeitet. Es enthält IT-Sicherheitsanforderungen und Empfehlungen für internetfähige Geräte im privaten oder kleingewerblichen Endkundenbereich wie z. B. IP-Kameras, Smart-TVs oder Smart Speaker.

Feststellung besteht nicht. Technische Richtlinien des Bundesamtes sollen stets Widerspruchsfreiheit mit internationalen, europäischen und nationalen Normen und Standards anstreben. Die Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, wird durch Rechtsverordnung nach § 10 Absatz 3 geregelt. Die Rechtsverordnung kann vorsehen, dass die für die jeweilige Produktkategorie maßgebliche Technische Richtlinie oder die branchenabgestimmten IT-Sicherheitsvorgaben eine abweichende Dauer festlegen können."

Über DIN

Das Deutsche Institut für Normung e. V. (DIN) ist die unabhängige Plattform für Normung und Standardisierung in Deutschland und weltweit. Als Partner von Wirtschaft, Forschung und Gesellschaft trägt DIN wesentlich dazu bei, die Marktfähigkeit von innovativen Lösungen durch Standardisierung zu unterstützen – sei es in Themenfeldern rund um die Digitalisierung von Wirtschaft und Gesellschaft oder im Rahmen von Forschungsprojekten. Rund 34.500 Experten aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein, den DIN als privatwirtschaftlich organisierter Projektmanager steuert. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fordern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen. Weitere Informationen unter www.din.de.

Über DKE

Die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE ist die in Deutschland zuständige Organisation für die Erarbeitung von Standards, Normen und Sicherheitsbestimmungen in den Themenfeldern Elektrotechnik, Elektronik und Informationstechnik. Als deutsches Mitglied in den internationalen und europäischen Organisationen für die Normung der Elektro- und Telekommunikationstechnik – IEC, CENELEC und ETSI – vertritt die DKE die deutschen Interessen bei der Erarbeitung und Weiterentwicklung der Internationalen und Europäischen Normen zum Abbau von Handelshemmnissen und zur weltweiten Öffnung der Märkte.