Normen und Standards

Ihre Instrumente zur Umsetzung politischer Ziele

SCHWERPUNKT: IT-SICHERHEIT

Die Cybersicherheitslage bleibt angespannt, Angriffe auf die Netzwerke von Unternehmen und Behörden legen immer öfter ganze Organisationen technisch lahm. Zur Stärkung der IT-Sicherheit in Deutschland hat die Bundesregierung sich weitreichende Ziele gesetzt, bei deren Umsetzung Normen und Standards unterstützen können. Sie definieren Terminologie, Schnittstellen, Sicherheits- und Qualitätsanforderungen und schaffen somit ein einheitliches Verständnis über Fachgebietsgrenzen hinweg. Durch Standards wird Vertrauen in Produkte, Anwendungen und Dienstleistungen geschaffen. Sie werden für Hersteller, Anwender und Verbraucher nachvollziehbar und überprüfbar.

Die Politik kann Normen und Standards als Instrumente zur Umsetzung politischer IT-Sicherheits-Ziele nutzen:

Politisches Ziel (s. Koalitionsvertrag von SPD, Grünen und FDP)	**So unterstützen Normen und Standards die Umsetzung**
Weiterentwicklung der Cybersicherheitsstrategie	▪ Die Vereinheitlichung technischer Anforderungen schafft eine wirkungsvolle Basis für vertrauenswürdige IT-Produkte. ▪ Standards öffnen Märkte und stärken so die Wettbewerbsfähigkeit deutscher Anbieter. ▪ Über die nationalen Normungsorganisationen werden deutscher Basistechnologien, Best Practices, Innovationen und Prüfverfahren in die europäische und internationale Normung eingebracht.
Weiterentwicklung des IT-Sicherheitsrechts	In Gesetzen und Verordnungen in Bezug genommene Normen und Standards schließen die Lücke zwischen rechtlichen Anforderungen und technischen Lösungen, die im Markt breit akzeptiert werden. Sie konkretisieren die rechtliche Anforderungen machen diese somit für Hersteller und Betreiber umsetzbar.
Recht auf Interoperabilität und Portabilität	Die Definition von Schnittstellen über die nationalen Normungsorganisationen schafft einheitliche Anforderungen und bildet die Basis für grenzübergreifende Interoperabilität durch eine enge Anbindung an die europäische und internationale Normung.
Digitale Souveränität durch offene Standards sichern	Normen sind offene Standards, für alle Marktteilnehmer leicht zugänglich und tragen insbesondere auf europäischer Ebene zur Harmonisierung des Digitalen Binnenmarktes und europäischer digitaler Souveränität bei. Deutschland sollte deshalb in der europäischen Normung gut aufgestellt sein.
IT-Sicherheit von digitalen und vernetzten Produkten	Im gemeinsamen Projekt „Qualitätsinfrastruktur (QI) digital“ arbeiten die Normungsorganisationen mit den an der QI beteiligten Akteuren aus Messwesen, Konformitätsbewertung, Zertifizierung und Akkreditierung zusammen, um das Qualitätsversprechen „Made in Germany“ digital und wettbewerbsfähig aufzustellen.

Deutschland ist Marktführer in der IT-Sicherheitsstandardisierung.

DIN und DKE leiten relevante Normungsgremien und bringen nationale Positionen in europäische und internationale Standards ein. Beispiele für Normen und Standards für IT-Sicherheit sind:

- DIN EN ISO/IEC 27001 „Informationstechnik – Sicherheitsverfahren – Informationssicherheits-managementsysteme – Anforderungen“
- DIN EN ISO/IEC 27002 „Leitfaden für Informationssicherheitsmaßnahmen“
- DIN EN ISO/IEC 27017 „Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste“
- DIN EN ISO/IEC 15408-Reihe „Evaluationskriterien für IT-Sicherheit“
- DIN EN 303645 „CYBER - Cybersecurity im Konsumenten-Bereich des Internets der Dinge: Mindestanforderungen“
- In Erarbeitung: DIN SPEC „KMU-geeignete IT-Sicherheitsberatung“

ANSPRECHPARTNERIN

Katja Krüger | Deputy Head of Government Relations
E-Mail: katja.krueger@din.de
Tel.: +49 30 2601 2439

Vor diesem Hintergrund empfiehlt DIN:

- Im Rahmen der Weiterentwicklung der Cybersicherheitsstrategie sollte ein Kapitel zur Standardisierung aufgenommen werden.
- Zur technischen Konkretisierung regulatorischer Rahmenbedingungen sollte auf bestehende, am Markt etablierte und breit akzeptierte Normen und Standards verwiesen werden.
- Wo bisher keine Standards existieren, sollten die nationalen Normungsorganisationen mit der Erarbeitung beauftragt werden. Eine aktive Mitarbeit der öffentlichen Hand in der Erarbeitung sollte sichergestellt werden.
- Der Aufbau von Parallelstrukturen zur Cybersicherheitsstandardisierung muss vermieden werden. Konsortialstandards und 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.

DIN als Wegbegleiter der Politik

Normen und Standards sind zentrale wirtschafts- und gesellschaftspolitische Instrumente. Sie ebnen deutschen Unternehmen und neuen Technologien den Weg auf internationale Märkte und stärken somit nachhaltig die Zukunfts- und Wettbewerbsfähigkeit Deutschlands.

Als unabhängige, privatwirtschaftlich organisierte Plattform koordiniert DIN Normung und Standardisierung in Deutschland und weltweit. Rund 36.000 Expert*innen aus Wirtschaft und Forschung, von Verbraucherseite und der öffentlichen Hand bringen ihr Fachwissen in den Normungsprozess ein. Die Ergebnisse sind marktgerechte Normen und Standards, die den weltweiten Handel fördern und der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft und Umwelt sowie der Sicherheit und Verständigung dienen.

Mit dem Normenvertrag von 1975 hat die Bundesrepublik Deutschland DIN als nationale Normungsorganisation und Vertreter Deutschlands in der europäischen und internationalen Normung anerkannt. Die Politik kann auf DIN als strategischen Partner zurückgreifen, um den gesetzlichen Regelungsrahmen möglichst schlank, effizient und flexibel zu gestalten.