Verband der TÜV e.V.

TÜV®

Verfasser
VdTÜV-Arbeitskreis Cybersecurity

Datum
03.Oktober 2015

VdTÜV-Stellungnahme zur Mitteilung der EU-Kommission „Strategie für einen digitalen Binnenmarkt für Europa“

Der VdTÜV e.V. begrüßt die von der EU-Kommission vorgelegte Mitteilung zur Strategie für einen digitalen Binnenmarkt (KOM(2015) 192). Sie hat einen ganz wesentlichen Einfluss auf den Standort und die Wettbewerbsfähigkeit Europas. Die Schaffung eines einheitlichen und austarierten digitalen Binnenmarkts ist notwendig, um die heutige Fragmentierung zu überwinden. Dies reduziert Kosten, schafft Synergien zwischen den Aktivitäten der EU-Staaten und steigert Europas Attraktivität als Investitionsstandort.

Nachfolgend legt der VdTÜV e.V. seine Standpunkte zur Strategie für einen digitalen Binnenmarkt dar. Die Mitteilung der EU-Kommission setzt entscheidende Eckpunkte im Bereich Verbraucherschutz, wobei aus Sicht des VdTÜV einige Aspekte für einen funktionierenden digitalen Binnenmarkt gerade auch aus Sicht der Wirtschaft zu ergänzen sind. Im Mittelpunkt stehen dabei IT-Sicherheit, Cloud-Computing, Normung und Interoperabilität sowie Weiterbildung. Zudem müssen diese Punkte in einer digital vernetzten Welt immer in enger Kooperation mit anderen Regionen, wie Ostasien und Nordamerika, gedacht werden.

Letztlich wird die konkrete Umsetzung der Digitalunion in einen soliden Rechtrahmen für ihren Erfolg entscheidend sein.

Zentrale Botschaften der VdTÜV-Stellungnahme

- Unabhängige, qualifizierte Prüfungen durch kompetente Stellen schaffen eine wirksame Verbesserung der Betreiber- oder Unternehmens IT-Sicherheitsarchitektur im digitalen Binnenmarkt.

- Ein EU-weites Rahmenwerk für Zertifizierungen im Bereich Informationssicherheit kann dazu beitragen, die digitale Souveränität der EU, also die Sicherheit der Datenkommunikation, besser zu gewährleisten.

- Eine europäische Cloud-Initiative muss klare Festlegungen über die Sicherheits- und Qualitätsanforderungen sowie den Rechtsrahmen von Cloud-Computing schaffen.

- IT-Sicherheit muss in der Normensetzung so verankert werden, dass sie künftig bereits als ein wesentliches Leistungsmerkmal des Entwicklungs- und Nutzungsprozesses verstanden wird (*safety & security by design*).

- Die berufliche Weiterbildung muss zu einem integralen Bestandteil einer digital durchdrungenen Arbeitswelt und der Personalentwicklung werden. Denn erst die Sensibilität der Nutzer für Sicherheitsmaßnahmen und grundsätzliches Wissen über Cybersicherheit schaffen nachhaltigen Informationsschutz auf hohem Niveau.

1. VdTÜV-Position zu Kapitel 3.4. der Mitteilung: „Stärkung des Vertrauens und der Sicherheit bei digitalen Diensten und beim Umgang mit personenbezogenen Daten“

Die geplante Verabschiedung der **Richtlinie über die Netz- und Informationssicherheit (NIS-Richtlinie)** ist ein wichtiger Schritt zur Stärkung des Cybersicherheitsniveaus in der EU. IT-Sicherheit, die Vertrauen in kritische Infrastrukturen schafft, ist ein entscheidender Faktor für die Entwicklung einer digitalen Wirtschaft. In den noch anstehenden Verhandlungen sollte aus unserer Sicht besonderes Augenmerk auf die Verankerung konkreter Anforderungen und transparenter Regeln für die Durchführung von Sicherheitsüberprüfungen bei kritischen Infrastrukturen gelegt werden. Nach unserer Auffassung muss dabei vor allem die Unabhängigkeit und Kompetenz der Stellen sichergestellt sein, die mit der Durchführung der Sicherheitsüberprüfung betraut sind, um die Aussagekraft und Belastbarkeit der Überprüfung sicherzustellen. Unabhängige Prüfungen entlasten darüber hinaus Unternehmen, eigene Prüfkompetenzen aufbauen zu müssen. Zudem erzielen **unabhängige, qualifizierte Prüfungen kompetenter Prüf-, Zertifizierungs- und Zulassungsstellen entscheidende Impulse zu einer wirksamen Verbesserung der Betreiber- oder Unternehmens IT-Sicherheitsarchitektur.** In Analogie zum Beschluss über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten (768/2008/EC) regen wir daher an, grundsätzlich die Einbindung von unabhängigen und kompetenten Stellen für IT-Sicherheitsüberprüfungen in Hochrisikobereichen im digitalen Binnenmarkt einzuführen.

Zudem halten wir die Schaffung eines **EU-weiten Rahmenwerks für Zertifizierungen** im Bereich Informationssicherheit nach internationalen Standards für erforderlich. Effiziente Zulassungs- und Zertifizierungsprozesse für IT-Sicherheitsprodukte können erheblich dazu beitragen, die digitale Souveränität der EU, also die Sicherheit der Datenkommunikation, zu gewährleisten, ohne dabei eine Abschottung von globalen Märkten und Internetinfrastrukturen zu riskieren.

Die vorgeschlagene Gründung einer **öffentlich-privaten Partnerschaft für Cybersicherheit** auf dem Gebiet der Technologien und Lösungen für die Online-Netzsicherheit sehen wir positiv, um Investitionen in die digitale Transformation voranzutreiben. **Es fehlt jedoch eine klare Aussage über die geplante Ausrichtung und Zielsetzung der öffentlich-privaten Partnerschaften für Cybersicherheit.** Hierbei sollte eine breite Beteiligungsstruktur von kompetenten Partnern der Industrie, vor allem auch aus klein- und mittelständischen Unternehmen und industrienahen Dienstleistungen, Ziel sein. Erprobte EU-Förderprogramme wie Horizon2020, COSME und EFSI sowie der „Juncker-Plan“ könnten im Verbund genutzt werden.

Darüber hinaus vermissen wir auch eine Bezugnahme auf den Schutz **nicht-personenbezogener Daten**, die bei vernetzten Gegenständen und Maschinen des „Internets der Dinge“ meist automatisiert über Sensoren in großer Menge generiert werden. Diese sogenannten Maschinendaten sind für die digitale Transformation der Industrie und ihrer wirtschaftlichen Verwertungsmöglichkeiten von zentraler Bedeutung. Maschinendaten sind bis dato weder zivilrechtlich noch urheberrechtlich geschützt und können niemandem eindeutig zur ausschließlichen Nutzung und weiteren Verwertung zugeordnet werden. **Rechtliche Unsicherheiten und offene Fragen hinsichtlich der Interoperabilität und Standardisierung sind schädlich für die Entwicklung von neuen, datenbasierten Märkten.**

2. VdTÜV-Position zu Kapitel 4.1. der Mitteilung: „Aufbau einer Datenwirtschaft“

Der VdTÜV e.V. begrüßt die Ankündigung der EU-Kommission für eine europäische **Cloud-Initiative**.

Wir stimmen mit der Einschätzung der EU-Kommission überein, dass vor allem fehlendes Vertrauen in die Sicherheit von Cloud-Anwendungen viele Unternehmen davon abhält, ihre Daten online verfügbar zu machen. Die Entwicklung vertrauenswürdiger und sicherer Cloud-Dienste in der EU kann einen wirklichen Standortvorteil generieren. **Aus Sicht des VdTÜV e.V. sollte eine europäische Cloud-Initiative dafür klare Festlegungen über die Sicherheits- und Qualitätsanforderungen sowie den Rechtsrahmen von Cloud-Computing treffen.** Diese Anforderungen sollten zudem zeitnah in einer entsprechenden international abgestimmten Standardisierungsstrategie aufgegriffen werden.

In der Praxis hat sich bereits gezeigt, dass unabhängige und professionelle Zertifizierungen, gemäß international anerkannter Standards, eine entscheidende Orientierungshilfe für die Nutzer über die Qualität und Vertrauenswürdigkeit eines Cloud-Dienstes, seines Anbieters und aller nachgelagerten Prozesse wie Sicherheit, Infrastruktur, Verfügbarkeit sind. Zu wichtigen Sicherheits- und Qualitätsanforderungen an einen Cloud-Dienst, die auch vertraglich zwischen Provider und Nutzer festgehalten werden sollten, zählen die Lokalität und Trennung von Daten, Netzwerksicherheit und Zugriffskontrollen. Die Speicherung von Daten muss verschlüsselt erfolgen, um eine nachträgliche Personalisierung von Daten in einer gemeinschaftlich genutzten Cloud zu verhindern. Dabei sollte der Cloud-Dienst hinsichtlich der Kriterien Prozess- und Aufbauorganisation, Datensicherheit, Compliance/Datenschutz, einschließlich eines rechtskonformen Löschvorgangs nach Vertragsende, Datenportabilität und der Nutzerfreundlichkeit der Cloud kompetent von unabhängiger Seite zertifiziert werden. Der Cloud-Kunde erhält so eine belastbare Aussage zur Qualität, Performance und Sicherheit der Cloud, der Cloud-Anbieter so eine Chance zur positiven Abgrenzung im Wettbewerb.

3. VdTÜV-Position zu Kapitel 4.2. der Mitteilung „Steigerung der Wettbewerbsfähigkeit durch Interoperabilität und Normung“

Für die digital vernetzte Produktion, die Verkehrsmittel der Zukunft, das Smart Home oder auch das Gesundheitswesen spielen internationale Normen und Standards eine entscheidende Rolle. Viele Produkte können nur dann marktfähig werden, wenn sie sich reibungslos in weltweite Informations- und Kommunikationswerke eingliedern lassen. Der Ansatz einer europäischen **Normung**, wie in der Strategie für einen digitalen Binnenmarkt für Europa angeführt, kann aus Sicht des VdTÜV e.V. daher nur der erste Schritt sein. **Europäische Normung muss perspektivisch immer im Kontext internationaler Normungsarbeit und Normungsaktivitäten anderer Weltmarktregionen gesehen werden.**

Normen fördern u. a. die wirtschaftliche Durchdringung im Europäischen Binnenmarkt und helfen bei der Entwicklung neuer und verbesserter Produkte. Für den freien und fairen Welthandel sind sie unerlässlich. Diejenigen Unternehmen, die ihr Know-how zu neuen Technologien und die dafür notwendigen Rahmenbedingungen frühzeitig in die Normung einbringen, können so ihre Wettbewerbs- und Innovationsfähigkeit auf den Weltmärkten verbessern.

Die EU-Kommission kann eine proaktivere Rolle übernehmen und aus ihrer Sicht fehlende technische Normen und Standards benennen, die die Digitalisierung von Industrie- und Dienstleistungssektoren unterstützen. Grundlage für die Beauftragung einer europäischen Normungsorganisation ist die Verordnung (EU) Nr. 1025/2012 zur europäischen Normung. Es wäre sinnvoll, bereits auf nationale Empfehlungen und bereits existierende Normungsroadmaps der EU-Staaten sowie auf die zu erwartenden Ausarbeitungen europäischer Initiativen wie der im März 2015 gestarteten „Alliance for Internet of Things Innovations“ für industriespezifische Standards zurückzugreifen. Ferner können bereits existierende Standards, insbesondere internationaler Normungsergebnisse und globaler Industriestandards in die europäische Normung überführt werden. Im Bereich Cybersicherheit spielen sowohl für Office-IT Anwendungen als auch bei der Prozess- und Fabrikautomation IT-Sicherheitsmanagementsysteme und Kryptoalgorithmen eine zentrale Rolle. **IT-Sicherheit muss in der Normensetzung so verankert werden, dass sie künftig bereits als ein wesentliches Leistungsmerkmal des Entwicklungs- und Nutzungsprozesses verstanden wird (safety & security by design).**

Die EU-Kommission plädiert aus unserer Sicht richtigerweise dafür, den Abstimmungsprozessen mit allen interessierten Kreisen in den Normungsgremien Vorrang gegenüber de-facto-Standards oder interner Normen internationaler Unternehmen einzuräumen. Die Erarbeitung von Normen und Standards in den entsprechenden Gremien steht vor der Herausforderungen immer kürzerer Innovationszyklen in digital vernetzten Technologien und Anwendungen gerecht zu werden, sowie Normen mit unmittelbarem Marktbezug zu erstellen. Die Experten in den Normungsgremien sollten dabei auf bestehende Möglichkeiten einer flexibleren Arbeitsweise und geeignete Formate zur beschleunigten Veröffentlichung von Normen zurückgreifen. Dazu zählt beispielsweise die Erarbeitung von technischen Spezifikationen als Vorstufe späterer konsensbasierter Normen.

Darüber hinaus ist auch eine enge Zusammenarbeit zwischen Forschung und Wirtschaft zur Etablierung von Anwendungsbeispielen für digitale Technologien, Produkte und Dienste zielführend, die politisch so unterstützt werden kann, dass die europäischen Interessen mit Partnern anderer Weltmärkte konzertiert ausgestaucht werden können. Die Partner aus Wirtschaft und Forschung sollten sich zudem auf internationaler Ebene stärker als bisher in die entsprechenden Gremien (ISO, IEC, ETSI, IEEE, OASIS, W3C etc.) einbringen. Europas Politik und Unternehmen müssen mit ihrem ganzen Gewicht an der globalen Standardisierungsdebatte teilnehmen.

4. VdTÜV-Position zu Kapitel 4.3. der Mitteilung: „Eine inklusive digitale Gesellschaft“

Aus Sicht des VdTÜV e.V. sind verstärkte **Bildungsanstrengungen** eine zentrale Voraussetzung um die digitale Transformation positiv zu gestalten, d. h. die Beschäftigten aller Altersgruppen mittels Bildung und Qualifizierung zur Mitgestaltung dieses Wandels zu befähigen. Aus Perspektive der IT-Sicherheit genügen rein technische Maßnahmen nicht, Bedrohungen abzuwehren. Der Mensch muss für die Herausforderung Cybersicherheit nachhaltig gerüstet werden. Für Beschäftigte sind hierbei u. a. folgende vier Kompetenzen zentral: die Bereitschaft zum lebenslangen Lernen, interdisziplinäres Denken und Handeln, höhere IT-Kompetenz und die Fähigkeit zum permanenten Austausch mit Maschinen und vernetzten Systemen. **Die berufliche Weiterbildung muss zu einem integralen Bestandteil einer digital durchdrungenen Arbeitswelt und der Personalentwicklung werden.** Weiterbildung kann individualisiert am Arbeitsplatz unter Berücksichtigung der jeweiligen Bedarfe und der vorhandenen Qualifikation erfolgen.

Die Zuständigkeit für Bildungsfragen liegt bei den Mitgliedsstaaten, dennoch kann die EU-Kommission übergreifend und impulsgebend tätig werden. Die Qualität der Weiterbildungsmaßnahmen sollte beispielsweise durch europäisch harmonisierte Leistungs- und Anforderungsprofile definiert werden, nach denen sie jeweils unabhängig und wiederkehrend zertifiziert werden können. Dies schafft vor der Investitionsentscheidung Vertrauen in den Nutzen und ermöglicht eine aussagekräftige Vergleichbarkeit der Weiterbildungsmaßnahmen im Europäischen Binnenmarkt. Darüber hinaus kann so sichergestellt werden, dass die Zeit zwischen dem Aufkommen neuer Anforderungen an Qualifizierung und deren Integration in die jeweilige Weiterbildungsmaßnahme verkürzt wird.

Zudem wäre es zu begrüßen, wenn die EU-Kommission Anstrengungen für ein europaweites Bürger-Portal für IT-Sicherheit aufnimmt. **Denn erst die Sensibilität der Nutzer für Sicherheitsmaßnahmen und grundsätzliches Wissen über Cybersicherheit schaffen nachhaltigen Informationsschutz auf hohem Niveau.**