Gemeinsames Positionspapier der Verbände VDMA, VdTÜV und ZVEI zum „Cybersecurity Act“
(COM (2017) 477 final)

Der europäische Binnenmarkt bildet für die deutsche Industrie einen unverzichtbaren, stabilen und harmonisierten Wirtschaftsraum, in dem Unternehmen Produkte nach einheitlichen Regeln vermarkten können.

Eine Vielzahl von Produktsektoren regelt der europäische Gesetzgeber auf Basis des „New Legislative Framework“ (NLF oder früher „New Approach“). Dieses Regulierungsmodell ist die tragende Säule des europäischen Binnenmarktes. Der „New Approach“ wurde zur europäischen Harmonisierung der Produktanforderungen entwickelt, um technische Handelshemmnisse in Europa und international abzubauen.

Der NLF begrenzt die Gesetzgebung im Produktbereich auf die Festlegung der wesentlichen Anforderungen. Um Produkte auf dem europäischen Binnenmarkt in Verkehr zu bringen, müssen diese auf ihre Konformität mit den geltenden einschlägigen Anforderungen überprüft werden. Dabei hängt die Ausgestaltung der anzuwendenden Konformitätsbewertungsverfahren vom Risiko des Produktes ab. Die zur Verfügung stehenden acht Konformitätsmodule (von der Herstellerselbsterklärung bis zum Qualitäts-Audit) vereinen dabei in effektiver Weise den risikobasierten Ansatz mit der Flexibilität für die Herstellerunternehmen. Denn die Pflicht zur Erfüllung dieser Anforderungen liegt bei den Herstellern.

Die Verbände VDMA, VdTÜV und ZVEI stellen mit Besorgnis fest, dass die Akteure im europäischen politischen Prozess zunehmend dazu tendieren, den erfolgreichen NLF nicht mehr hinreichend konsequent und durchgängig anzuwenden oder bei bestimmten Fragestellungen sogar gravierend vom NLF abweichende, mithin systemfremde Regelungen treffen zu wollen. Im Hinblick darauf hat die deutsche Wirtschaft mit Blick auf eine sachgerechte und effiziente Produktregulierung in Europa wesentliche Kernanliegen in den Bereichen Konformitätsbewertung, Akkreditierung, Marktüberwachung, Stabilität des Regelwerkes und Normung formuliert.[1]

Im Rahmen der neuen Cybersicherheitsstrategie hat die Europäische Kommission im September 2017 den Entwurf einer Verordnung zur "EU Cybersecurity Agency" und zum „Cybersecurity Act“ vorgelegt.

Unter Berücksichtigung der Grundprinzipien der Europäischen Produktregulierung nach dem NLF sollte auch der „Cybersecurity Act“ den folgenden Anforderungen genügen:

[1] https://bdi.eu/media/themenfelder/umwelt/Positionspapier_EU-Binnenmarkt_DE.PDF

1. Wirtschaftsgetragene Konformitätsbewertung beibehalten

2. Bewahrung der Flexibilität und Innovationskraft für die Unternehmen durch eine risikobasierte Anwendung der Mittel der Herstellerselbsterklärung oder der unabhängigen Drittprüfung, wie sie im NLF verankert sind.

3. keine behördlichen Produktzulassungsverfahren

4. Akkreditierungssystem stärken – keine nationalen Sonderwege

5. staatliche Marktüberwachung effizient gestalten, um die Konformität der Produkte sowie ein *Level Playing Field* zwischen Herstellern und Importeuren zu gewährleisten

6. Stabilität, Kohärenz, und Klarheit des europäischen Regelwerkes zur Produktregulierung gewährleisten

7. Europäische Normung marktorientiert, privatwirtschaftlich organisiert und finanziert gestalten – keine politischen Einflussnahmen.

Um eine maximale Konsistenz und Kohärenz mit den parallel anzuwendenden sektoralen Vorschriften der Europäischen Produktregulierungen zu gewährleisten, sollte der Cybersecurity Act mit Blick auf die Cybersicherheitszertifizierung möglichst weitgehend den Prinzipien des NLF folgen und das gesamte Spektrum der Konformitätsbewertungsverfahren ermöglichen. Somit lassen sich folgende Forderungen ableiten:

- Die Zertifizierung bzw. Selbstbewertung, also die Konformitätsbewertung der IKT-Produkte, hat einem risikobasierten Ansatz zu folgen.
- Sie sollte grundsätzlich privatwirtschaftlich organisiert und getragen sein, außer für den etablierten Bereich der Common Criteria.
- Die Schaffung von parallelen, unerprobten Ansätzen zur Produktregulierung ist zu vermeiden, da dies zu unnötigem Aufwand und Unsicherheit für die Unternehmen führt.
- Damit internationale Akzeptanz und Kompatibilität gewährleistet ist, sollte die Kompetenz der Konformitätsbewertungsstellen im Zuge einer Akkreditierung nachgewiesen werden. Diese ist Basis ihrer Benennung, die damit einen rein formalen Akt darstellt.
- Bei der Ausgestaltung der cybersecurity schemes sollte auf den technischen Sachverstand der Wirtschaftsakteure gesetzt werden, insbesondere sollten Grundprinzipien der europäischen und internationalen Normung gewahrt werden sowie bestehende Normen angemessene Berücksichtigung finden. Zusätzlich sind die Wirtschaftsakteure durch transparente, effektive und diskriminierungsfreie Prozesse jeweils einzubinden. Wenn möglich, sollte auf die etablier-

ten Normungsprozesse, die diese Anforderungen tagtäglich erfüllen, zurückgegriffen werden.

- Behörden sollten im Zuge der Zertifizierung Aufsichtsfunktionen übernehmen und allenfalls im Hochsicherheitsbereich entsprechend ihrer hoheitlichen Schutzfunktionen im Zertifizierungsprozess eine operative Rolle einnehmen.
- Zur Vermeidung von Interessenkonflikten bedarf es einer klar abgegrenzten Rollenverteilung in der Verordnung. Wer prüft und zertifiziert, wer notifiziert und wer akkreditiert, muss eindeutiger festgelegt werden. Grundsätzlich dürfen die verschiedenen Akteure jeweils nur eine Rolle wahrnehmen.

Berlin, 27. Juli 2018