Verbund der Telekommunikations-Endgerätehersteller (VTKE)
Alt-Moabit 90a ▪ 10559 Berlin
0173 – 628 62 44 ▪ info@vtke.de ▪ www.vtke.de

5. Dezember 2017

Stellungnahme zum
Vorschlag für eine Verordnung über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit")
(COM (2017) 477 final)

Mit der immer weiteren Digitalisierung unserer Gesellschaft und Wirtschaft steigt auch die Zahl potenzieller Sicherheitsbedrohungen. Vor diesem Hintergrund nimmt die Bedeutung von IT- und Cybersicherheit stetig zu. Der Verbund der Telekommunikations-Endgerätehersteller (VTKE) begrüßt daher ausdrücklich die Anstrengungen der Europäischen Union zur Schaffung von mehr Cybersicherheit.

Angesichts der Tatsache, dass Cyberbedrohungen nicht an nationalen Grenzen Halt machen, betrachten wir ein gesamteuropäisches Vorgehen als durchaus sinnvoll. Nationale Lösungsansätze werden der grenzüberschreitenden Dynamik von Cybersicherheit bzw. Cybersicherheitsbedrohungen nicht gerecht. Darüber hinaus wirkt ein gesamteuropäischer Ansatz zur Erhöhung der Cybersicherheit einer Marktfragmentierung entgegen und schafft gleiche Wettbewerbsvoraussetzungen für alle Marktakteure.

Insofern ist es auch unserer Sicht nur konsequent, dass mit dem Inkrafttreten des europäischen Systems für die Cybersicherheitszertifizierung vergleichbare nationale Systeme unwirksam werden. Nur so kann der Zersplitterung von Zertifizierungsinitiativen innerhalb der Europäischen Union effektiv entgegengewirkt und ein einheitliches Cybersicherheitsniveau in allen EU-Mitgliedsstaaten erreicht werden. Dies wiederum stärkt die Europäische Union als Ganzes im Bereich der Sicherheit in der Informations- und Kommunikationstechnik, insbesondere auch gegenüber anderen Akteuren auf dem globalen Markt.

Wir begrüßen außerdem, dass die Cybersicherheitszertifizierung freiwillig sein soll. Die Freiwilligkeit lässt den Unternehmen, die IKT-Produkte und –Dienste herstellen, ausreichende Entscheidungsspielräume, ermöglicht ihnen jedoch gleichzeitig, die Qualität und das Sicherheitsniveau ihrer Produkte auf dem Markt bzw. gegenüber ihren (potenziellen) Kunden zu kommunizieren.

Studien, Statistiken und die konkrete Praxiserfahrung zeigen, dass viele unterschiedliche Produktgruppen aus dem Bereich der Informations- und Kommunikationstechnologie mit Cyberbedrohungen konfrontiert werden. Es ist aus unserer Sicht daher richtig und wichtig, dass das durch die Verordnung geschaffene europäische Rahmen für die Cybersicherheitszertifizierung von Anfang an eine breite Produktpalette, nämlich alle IKT-Produkte und –Dienste, in den Blick nimmt. Maßnahmen zur Erhöhung der Cybersicherheit müssen diese Vielfalt abbilden und auf die dynamisch verändernden (technischen) Gegebenheiten der Produkte anwendbar/anpassbar sein. Vor diesem Hintergrund muss unseres Erachtens gewährleistet werden, dass für alle Produktgruppen möglichst

gleiche, grundlegende Cybersecurity-Anforderungen festgelegt werden, denn nur so kann eine echte Vergleichbarkeit für den Verbraucher geschaffen werden. Statt separate Systeme für die Cybersicherheitszertifizierung für einzelne Produktkategorien auszuarbeiten, sollte daher überlegt werden, generische Cybersecurity-Standards zu definieren, denen alle IKT-Produkte und –Dienste entsprechen müssen. Dies hätte wiederum auch den Vorteil, dass solche generischen Cybersecurity-Anforderungen wesentlich flexibler sind und sich daher wesentlich leichter an den äußerst dynamischen technologischen Wandel anpassen lassen.

Berücksichtigt werden muss aus unserer Sicht auch, dass Zertifizierungsprozesse stets vergangenheitsbezogen sind. Im Umfeld der Informations- und Kommunikationstechnologie, das sich äußerst dynamisch entwickelt, kann ein Produkt oder Dienst am Ende des Zertifizierungsprozesses (sicherheits-)technisch bereits überholt sein. Statt statischer technischer Sicherheitsanforderungen, die lediglich einen kurzen Augenblick in der Entwicklung der Cybersicherheit abbilden können, sollten die Cybersicherheitsanforderungen eher prozessual orientiert sein. Auf diese Weise passen sich die Vorgaben flexibel auf die sich ändernden (technischen) Gegebenheiten an und können gleichzeitig die Cybersicherheitsrisiken der IKT-Produkte und –Dienste reduzieren.

Allerdings darf aus unserer Sicht nicht außer Acht gelassen werden, dass jede noch so durchdachte Maßnahme keine absolute Sicherheit der IKT-Produkte und –Dienste erreichen kann. Ein großer Teil der europäischen Hersteller und Anbieter von IKT-Produkten und –Diensten hält bereits heute aus eigenem Interesse sehr hohe Cybersicherheitsstandards ein. Bei der Erarbeitung von Cybersicherheitsanforderungen kann es aus unserer Perspektive daher nur darum gehen, das größtmögliche Cybersicherheitsniveau zu erreichen und die Cybersicherheitsrisiken so weit wie möglich zu verringern. Eine Cybersicherheitszertifizierung, die der breiten Öffentlichkeit Vertrauen in die Cybersicherheit von IKT-Produkten und –Diensten vermitteln soll, muss dies in seiner Kommunikation gegenüber den Anwendern berücksichtigen. Dass es keine absolute Cybersicherheit geben kann soll selbstverständlich aber auch nicht bedeuten, dass das Gros der Hersteller und Anbieter von IKT-Produkten und –Diensten nicht mit großen Mühen aus eigenem Antrieb die höchstmögliche Sicherheit ihrer Produkte anstrebt.

Überdies halten wir die vorgeschlagene Beteiligung der betroffenen Industrieakteure für unzureichend. Aus dem Verordnungsentwurf wird nicht klar, welchen Umfang die Konsultation „alle[r] in Frage kommenden Interessenträger“ (vgl. Art. 44 Nr. 2.) haben soll. Darüber hinaus sieht der Verordnungsentwurf keine Beteiligung der Industrie an der Arbeit der Europäischen Gruppe für die Cybersicherheitszertifizierung vor, die nicht unerheblichen Einfluss auf das europäische System für die Cybersicherheitszertifizierung haben soll. Wir sind der Meinung, dass die Akzeptanz der Cybersicherheitszertifizierung mit stärkerer Beteiligung der betroffenen Branchen sowohl hinsichtlich der Konsultation zur Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung als auch bei der Arbeit der Europäischen Gruppe für die Cybersicherheitszertifizierung signifikant erhöht werden könnte.

Neben der adäquaten Ausgestaltung der Cybersicherheitsanforderungen ist die korrekte Einhaltung dieser eine Voraussetzung für den Erfolg der Cybersicherheitszertifizierung. In Artikel 54 des

Verordnungsentwurfs wird vorgeschlagen, dass die Vorschriften über Sanktionen bei Verstößen gegen die festzulegenden Cybersicherheitsvorgaben von den Mitgliedsstaaten erlassen werden sollen. Diese sollen „wirksam, verhältnismäßig und abschreckend“ sein. Wir möchten in diesem Zusammenhang anregen, dass die Vorschriften über Sanktionen zentral – und durch die einzelnen EU-Mitgliedsstaaten – festgelegt werden. Auf diese Weise würden auch hinsichtlich der Sanktionsmechanismen gleiche Wettbewerbsvoraussetzungen für alle Marktakteure innerhalb der Europäischen Union geschaffen. Gleichzeitig würde verhindert, dass über die Sanktionsart und –höhe in den einzelnen Mitgliedsstaaten Unterschiede im Cybersicherheitsniveau ermöglicht werden.

Die Cybersicherheitszertifizierung spielt nach Ansicht der EU-Kommission eine wichtige Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte und –Dienste zu stärken und deren Sicherheit zu erhöhen. Um dieses Ziel zukünftig zu erreichen, sollten unseres Erachtens die vorangehend genannten Anmerkungen berücksichtigt werden.

Letztlich sind wir aber auch der Auffassung, dass eine effektive Erhöhung der Cybersicherheit nur durch das koordinierte Zusammenspiel aller Beteiligter – Gerätehersteller, Diensteanbieter, Infrastrukturbetreiber, Anwender usw. – erreicht werden kann.

Bei Fragen und/oder für weitere Informationen stehen wir Ihnen jederzeit gerne zur Verfügung.