06.07.2018

(Dr. Dennis-Kenji Kipker, Universität Bremen)

**Bewertung der Stellungnahme des IMCO-Ausschusses des EP zum Entwurf einer EU-Cybersecurity-Verordnung**

Am 22.05.2018 hat der Ausschuss für den Binnenmarkt und Verbraucherschutz (IMCO) des Europaparlaments seine Stellungnahme zu dem "Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates 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")" - besser bekannt auch als "Cybersecurity-Verordnung" - veröffentlicht. Der neue europäische Rechtsakt zur Cybersicherheit basiert auf zwei Grundpfeilern: Einem ständigen und stärkeren Mandat der ENISA, sowie der Einführung eines EU-Rahmens zur Cybersicherheitszertifizierung, um sicherzustellen, dass Produkte der Informations- und Kommunikationstechnologie sowie entsprechende Dienste die dafür relevanten Cybersicherheitskriterien auf einheitliche Weise erfüllen.

**Rechtspolitische Zusammenhänge**

Nach dem Inkrafttreten der EU NIS-RL im Jahr 2016 wurde von der Europäischen Kommission im Herbst 2017 die neue EU-Cybersicherheitsstrategie präsentiert, die das primäre Ziel verfolgt, die Abwehrfähigkeit der EU gegenüber Cyberangriffen in einem weitergehenden Maße als bisher zu stärken. In diesem Zuge erfolgte am 13.09.2017 die Entwurfsvorstellung der europäischen Cybersecurity-Verordnung, zu dem der EU-Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) zunächst Stellung nahm. Wesentliche Aspekte seiner Stellungnahme betrafen die so genannten "Baseline IT security requirements" für alle IT-Produkte, die in der EU verkauft oder aus dieser heraus exportiert werden sollen. Daneben wurden seinerzeit Aspekte einer stärkeren Verzahnung von IT-Sicherheit und Datenschutz, die Bekämpfung von Cybercrime und IT-Sicherheitslücken sowie eine erweiterte Einbindung der Normung und Standardisierung diskutiert. Die jüngste Stellungnahme des IMCO-Committee enthält ebenso zahlreiche Änderungsvorschläge, die im Folgenden unter Relevanzgesichtspunkten aufgegriffen werden.

**Konformitätsbewertung durch Dritte und Konformitäts-Eigenerklärung**

Einer der Hauptbestandteile des Entwurfes der EU Cybersecurity-Verordnung ist die so genannte "Konformitätsbewertung", innerhalb derer festzustellen ist, ob IKT-Produkte oder -Dienste die an die Cybersicherheitsmerkmale anzulegenden Anforderungen erfüllen. Die durchzuführende Konformitätsbewertung soll durch einen Dritten, der nicht Produkthersteller oder Diensteanbieter ist, erfolgen. Dies kann beispielsweise durch zu diesem Zweck eingerichtete und akkreditierte Konformitätsbewertungsstellen geschehen. Neben dem Vorschlag des IMCO-Ausschusses, die Prüfung nunmehr nicht nur auf Cybersicherheitsmerkmale, sondern auch auf Cybersicherheitsverfahren zu beziehen, wird ebenfalls der Gedanke eingebracht, Konformitäts-Eigenerklärungen durchzuführen. Hierunter zu verstehen ist die Erklärung eines Herstellers, dass sein IKT-Prozess, -Produkt oder -Dienst mit einem einschlägigen europäischen System zur Cybersicherheitszertifizierung im Einklang steht. In diesem Zusammenhang ist jedoch vorrangig zu bestimmen, in welchen konkreten Bereichen eine Konformitäts-Eigenerklärung überhaupt möglich ist und somit zulässig sein kann. Denn für die Funktionsfähigkeit eines solchen Systems ist es nach Auffassung des IMCO-Ausschusses notwendig, dass die von den Nationalstaaten einzurichtenden Behörden für Cybersicherheitszertifizierung die Konformitäts-Prüfungen, insbesondere die Eigenerklärungen der Unternehmen, anhand der von der Cybersecurity-Verordnung aufgestellten Anforderungen kontrollieren. Im Falle der Konformitäts-Eigenerklärung eines Herstellers müssten die Behörden somit zusätzliche Maßnahmen ergreifen können, um die internen Verfahren des Unternehmens zu prüfen, mit denen sichergestellt werden soll, dass die Produkte oder Dienste die Anforderungen des europäischen Systems für die Cybersicherheitszertifizierung erfüllen.

Da eine Zertifizierung von IKT-Produkten und -Diensten jedoch nicht zwingend aussagt, dass diese tatsächlich und in jedem Falle sämtliche an die Cybersicherheit anzulegenden Kriterien erfüllen, fordert das IMCO-Committee explizit und weitergehend als der Verordnungsentwurf, dass Verbraucher über die Restrisiken der Zertifizierung aufzuklären sind, indem unter anderem darauf hingewiesen wird, dass die entsprechenden Produkte und Dienste nur auf die Übereinstimmung mit beispielsweise in technischen Normen und Standards festgelegten Anforderungen an die Cybersicherheit hin überprüft wurden.

**Umfassende Einbeziehung von Nutzergruppen, Interessengemeinschaften, Vereinigungen sowie der technischen Normung und Standardisierung**

Transparenz, Beteiligung und angemessene Verfahrensvorgaben sind von hoher Bedeutung für die Einrichtung und das Funktionieren eines vertrauenswürdigen und effektiven europäischen Cyber-Sicherheitsrahmens. Zu diesem Zweck schlägt der IMCO-Ausschuss vor, eine ständige Gruppe relevanter Interessenvertreter zu installieren, wozu nach Auffassung des Ausschusses unter anderem auch die Normungsorganisationen der jeweiligen Mitgliedsstaaten gehören sollen. Der ENISA kommt dabei die Aufgabe zu, das neue EU-Zertifizierungssystem in Zusammenarbeit mit der Gruppe der Interessenvertreter auszuarbeiten. Durch diesen gegenseitigen Prozess wird nach Auffassung des IMCO-Committees eine Konformität der Zertifizierung mit bestehenden Normen erreicht. Nach der in der Stellungnahme vertretenen Auffassung handelt es sich bei Normen um freiwillig umzusetzende, marktorientierte Instrumente, die technische Anforderungen und Leitlinien beinhalten und aus einem offenen, transparenten und integrativen Verfahren hervorgehen. Der ständigen Gruppe der relevanten Interessenvertreter sollen auch Verbrauchergruppen und -verbände angehören, sodass im Rahmen des Entwurfes des Zertifizierungssystems auch die Bedenken und Bedürfnisse der Endanwender in ausreichendem Maße Berücksichtigung finden können. Nicht zuletzt trifft die Gruppe der Interessenvertreter die Aufgabe, die Anforderungen der Cybersicherheit fortzuentwickeln, indem gegenwärtige und künftige Risiken identifiziert und ebenso in die Forschung in diesem Bereich einbezogen werden.

**Mindestsicherheitsstandards für IT-Produkte, die in der EU verkauft oder von dort exportiert werden, sowie Gewährleistung von IT-Sicherheit für den gesamten Produkt-Lebenszyklus und Umgang mit Backdoors**

Gemäß den Ausführungen des IMCO-Committees trifft die ENISA ferner die Aufgabe - ähnlich den "Baseline IT-security requirements", die auch schon vom LIBE-Committee aufgegriffen wurden -, Leitlinien zu Mindestsicherheitsstandards für IT-Produkte zu entwerfen, die in der Union in den Verkehr gebracht oder aus dieser exportiert werden. Die Hersteller haben in diesem Zusammenhang die Möglichkeit, schriftlich zu erklären, dass ihre Produkte weder Hardware-, Software-, oder Firmware-Komponenten mit bekannten ausnutzbaren Sicherheitslücken enthalten, zudem keine nicht veränderbaren oder nicht verschlüsselten Passwörter oder Zugangscodes verwendet werden, die nicht fähig sind, aus vertrauenswürdiger Quelle stammende und korrekt authentifizierte Sicherheitsupdates anzunehmen, und dass zur Reaktion des Verkäufers bei einem betroffenen Gerät eine angemessene Rangfolge von Abhilfemaßnahmen gehört. Die Verkäufer von IT-Produkten sollen die Endnutzer ferner über den Zeitpunkt unterrichten, zu welchem die Unterstützung für ein Gerät endet. Durch vorgenannte Transparenzmaßnahmen soll das Vertrauen der Unionsbürger in die Cybersicherheitsstrategie der EU insgesamt gestärkt werden.

Recht eng verbunden mit der Definition von Mindestsicherheitsstandards für IT-Produkte ist das Ziel, die Prinzipien von "Security by Design" sowie von "Privacy by Design" konsequent umzusetzen und umfassend in Produkte und Dienste zu integrieren. Hierzu soll das europäische Zertifizierungssystem für Cybersicherheit laut der Auffassung des IMCO-Ausschusses so ausgestaltet werden, dass alle hierdurch betroffenen Akteure die IT-Sicherheitsanforderungen in allen Phasen des Produkt- oder Dienstlebenszyklus umsetzen.

Eine umfassende Auseinandersetzung mit europaweiten Fragen der Cybersicherheit setzt darüber hinaus die Bestimmung von Anforderungen im Umgang mit Backdoors in IKT-Produkten und -Diensten voraus. Hierzu soll die Kompetenz der ENISA dahingehend erweitert werden, dass diese in Zusammenarbeit mit den nationalen Zertifizierungsbehörden Verfahren zur "Cyberhygiene" und zur Verhinderung ebensolcher Backdoors entwickelt.

**Explizite Einbeziehung des Datenschutzes unter dem Regime der EU DS-GVO, Regelungen zum Umgang mit Data Breaches**

Fragen der Cybersicherheit und des Datenschutzes wurden in bisher verfolgten Regulierungsansätzen im Wesentlichen losgelöst voneinander betrachtet. Dies soll ausgehend von der IMCO-Stellungnahme in Zukunft anders gehandhabt werden. Dem Vorschlag entsprechend ist das Mandat der ENISA im Hinblick auf die Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts auch auf den Datenschutz auszuweiten. So berät die Behörde den Europäischen Datenschutzausschuss bei der Erstellung von Leitlinien, die die technischen Voraussetzungen für die Nutzung von zu IT-Sicherheitszwecken notwendigen personenbezogenen Daten regeln, um damit beispielsweise Angriffe gegen IT-Systeme abzuwehren. In diesem Kontext sollen auch die Regelungen der EU-DSGVO einbezogen werden. Soweit der IMCO-Stellungnahme gefolgt wird, verwaltet die ENISA zudem nicht nur die Daten zu Cybersicherheitsvorfällen, sondern auch von Datenschutzverletzungen und hält Empfehlungen zur Datensicherheit vor.

Signifikante IT-Sicherheitsvorfälle können sich zudem nicht nur auf die M2M-Kommunikation, sondern auch auf Datenschutzverletzungen beziehen. Kommt es deshalb zu einer erheblichen Sicherheitsbeeinträchtigung, so hat die ENISA gemäß der Stellungnahme des IMCO-Committees die Pflicht, diese auch für Data Breaches über ein eigenes Portal auszuweisen. Die ENISA bündelt hierzu die Informationen verschiedener Organe, Einrichtungen und sonstiger Stellen der EU.

**Einführung unterschiedlicher IT-Sicherheitsstufen für IKT-Produkte und Dienste**

Das IMCO-Committee kritisiert in seiner Stellungnahme, dass bisherige internationale und nationale IT-Sicherheits-Zertifizierungen unter Berücksichtigung der von ihnen für Produkte und Dienste geführten Vertrauenswürdigkeitsstufen unterschiedliche Anforderungen stellten. Um dieser Entwicklung entgegenzutreten, soll die ENISA für IKT-Produkte und -Dienste in Zukunft einheitliche Vertrauenswürdigkeitsstufen publizieren, wobei die Cybersicherheitszertifizierung jedes Produkt sowie jeden Dienst einer bestimmten Sicherheitsstufe zuordnet. Damit einhergehend ändert sich, der IMCO-Stellungnahme folgend, auch die vorherige Bezeichnung der Sicherheitsstufen: Die niedrigste erste Stufe ist als "funktional sicher" zu beschreiben, was ein "angemessenes Maß" an Vertrauen in die IT-Sicherheitsstruktur impliziert - bezogen auch auf die IT-Sicherheitseigenschaften, die im Rahmen der Cybersicherheitszertifizierung überprüft werden. Die zweite Stufe "im Wesentlichen sicher" bildet demgegenüber ein mittleres Maß an Vertrauen ab, wohingegen die dritte Stufe "äußerst sicher" für ein erhöhtes Maß an Sicherheitsvertrauen in Produkte und Dienste steht. Eine Feinabstufung im Rahmen dieser Einteilung wird ebenfalls in Betracht gezogen. Deutlich gemacht werden soll darüber hinaus aber auch, dass selbst ein cybersicherheitszertifiziertes Produkt keine absolute Sicherheit genießt. Hierzu schlägt das IMCO-Committee eine bei der ENISA zu führende Checkliste vor, aus der ersehen werden kann, welche Cybersicherheitsrisiken ein IKT-Produkt oder -Dienst grundsätzlich abwehren kann, sodass sich Nutzer und Verbraucher über die generellen IT-Sicherheitsrisiken einer Nutzung schon im Vorfeld informieren können.

**Zeitliche Gültigkeitsbegrenzungen der Zertifizierung, ex-post-Überprüfungen sicherheitszertifizierter Produkte und Services**

Soweit eine Cybersicherheitszertifizierung stattfindet, geht der IMCO-Vorschlag dahin, die Geltungsdauer der ausgestellten Zertifikate zeitlich zu begrenzen. Darüber hinaus wird die Empfehlung gegeben, die ENISA zu regelmäßigen ex-post-Überprüfungen der ausgestellten Zertifikate auf deren Einhaltung hin zu ermächtigen.

**Erstellung einer "Priority List" der für eine Cybersicherheitszertifizierung relevanten IKT-Produkte und -Dienste**

Laut des IMCO-Committees soll die ENISA zukünftig die Aufgabe zur Erstellung einer Prioritätenliste erhalten, aus der sich infolge regelmäßiger Updates entnehmen lassen soll, für welche IKT-Produkte und -Dienste sie den notwendigsten Bedarf für eine Cybersicherheitszertifizierung sieht. Die Festlegung der Liste erfolgt in Zusammenarbeit mit der ständigen Gruppe der Interessenvertreter und der Europäischen Gruppe für die Cybersicherheitszertifizierung, zusammengesetzt aus den nationalen Zertifizierungsbehörden. Der Entwurf der Auflistung erfolgt als Bestandteil eines Arbeitsprogramms, zu welchem auch die Bestimmung spezifischer Einzelmaßnahmen zur kohärenten Durchsetzung der Cybersecurity-Verordnung im Unionsgebiet gehört.

**Einführung eines Peer-Review-Verfahrens für die nationalen Zertifizierungsbehörden**
Die nationalen Zertifizierungsbehörden sollen, so der Vorschlag des IMCO-Ausschusses, regelmäßigen "Peer Reviews" in Bezug auf ihre Tätigkeitsfelder unterfallen. Diese "Peer Reviews" sollen mindestens alle fünf Jahre durch zwei andere nationalstaatliche Zertifizierungsbehörden und durch die Europäische Kommission, aber auch unter Beteiligung der ENISA, durchgeführt werden. Mit dem "Peer Review" wird ein Prozess beschrieben, in dem die Zertifizierungsverfahren der nationalen Behörden und auch die fachliche Eignung des Personals, die Ordnungsmäßigkeit der Kontrollen und die Prüfmethodik sowie die Richtigkeit der Ergebnisse der Zertifizierungsbehörden überprüft werden, sodass europaweit einheitliche Verfahren für und Anforderungen an die Cybersicherheitszertifizierung bestehen. Um eine Vergleichbarkeit der "Peer Reviews" untereinander zu gewährleisten, ist die EU-Kommission dazu aufgefordert, ihre Methodik in einem konkreten Plan festzulegen.

**Abschlussbetrachtung**
Entgegen mancher Erwartung hat der IMCO-Ausschuss des Europäischen Parlaments im Vergleich zum ursprünglichen Kommissionsentwurf zahlreiche Änderungsvorschläge der EU Cybersecurity-Verordnung hervorgebracht, worunter sich auch verschiedene interessante und neuartige Ansätze finden. In besonderem Maße hervorzuheben ist zunächst der Gedanke, abweichend vom "klassischen" Muster nicht nur eine Konformitätsbewertung durch dritte, akkreditierte Stellen durchzuführen, sondern auch die Eigenerklärung durch Unternehmen in bestimmten Bereichen zu ermöglichen, wodurch weitere Anreize zur aktiven Befassung mit Fragen der unternehmensinternen Compliance zur Cybersicherheit geschaffen werden. Die Stellungnahme nimmt in einer Gesamtwertung die gesetzlichen Cybersicherheitsanforderungen überdies nicht zurück, sondern erweitert diese vielmehr in begrüßenswerter Weise, indem in Linie mit der vorangegangenen LIBE-Stellungnahme Mindestsicherheitsstandards für IT-Produkte in oder aus dem europäischen Raum bestimmt werden sollen und das Ziel definiert wird, aktive Cybersicherheit als einen Prozess zu begreifen, der eine umfassende Betrachtung über den gesamten Produkt- und Dienstleistungslebenszyklus hinweg erfordert.

Darüber hinaus ist es wichtig, Cybersicherheit von Beginn an als multidisziplinäre Aufgabe zu begreifen, die in rechtspolitischer und technologischer Hinsicht die Vielzahl betroffener Stakeholder aktiv einbezieht. Der durch die IMCO-Stellungnahme abgewandelte europäische Gesetzesentwurf zur Cybersecurity-Verordnung berücksichtigt auch diese Anforderung hinreichend, indem er an verschiedenen Stellen die Rolle von Nutzergruppen, Interessengemeinschaften, Vereinigungen sowie der technischen Normung und Standardisierung hervorhebt.

Positiv hervorzuheben ist ebenso, dass die Stellungnahme des IMCO-Committees nunmehr auch explizit auf Datenschutzaspekte Bezug nimmt und Regelungen zum Umgang mit Data Breaches vorsieht. In der Vergangenheit - so zum Beispiel auch im deutschen ITSiG - wurden die Themen Datenschutz, Datensicherheit und IT- bzw. Cybersicherheit im Wesentlichen losgelöst voneinander gehandhabt. Mit einem solchen Vorgehen wird aber nicht berücksichtigt, dass die vorgenannten Bereiche in einem engen sachlichen Zusammenhang zueinander stehen, so kann es zum Beispiel notwendig sein, personenbezogene Daten zu Zwecken der IT-Sicherheit auszuwerten, und effektive Datensicherheit kann nicht ohne hinreichende technisch-organisatorische Maßnahmen der IT-Sicherheit gewährleistet werden, sodass hier ein Bedürfnis für entsprechende spezialgesetzliche Regelungen besteht. Indem die IMCO-Stellungnahme auch diesen Aspekt adressiert, trifft sie eine wesentliche Neuausrichtung des Cybersecurity-Rechts, um dieses auf einheitliche Weise fortschrittlich und zukunftsweisend zu gestalten.