Dennis-Kenji Kipker/Dario Scholz EU-Parlament verabschiedet EU Cybersecurity Act

MMR-Aktuell 2019, 414986

Am 12.3.2019 hat das *EU-Parlament* die Cybersecurity-Verordnung (Cybersecurity Act) verabschiedet, nachdem bereits im Dezember 2018 im Trilog zwischen *Rat*, *Kommission* und *Parlament* eine Einigung über die wesentlichen Inhalte der Verordnung erzielt wurde. Kerninhalt des neuen Rechtsakts bleibt die Einführung eines dualen europäischen Systems zur Zertifizierung der Cybersicherheit und die Umstrukturierung der *ENISA*.

Als übergeordnete Zwecke werden u.a. der Schutz des digitalen EU-Binnenmarkts und die Erleichterung des ausländischen Marktzugangs durch Anerkennung von Cybersicherheitszertifizierungen in allen Mitgliedstaaten genannt. Über die Verordnung finden darüber hinaus die Prinzipien „Security by Default" und „Security by Design" einen Anker in der europäischen Gesetzgebung, sodass dieser schon durch die DS-GVO für den Datenschutz vorgegebene Maßstab nunmehr auch explizit für die IT-Sicherheit Berücksichtigung findet. Auch wird umfassender als bisher externer Sachverstand eingebunden. Hervorhebenswert ist in diesem Zusammenhang die Gründung einer *ENISA-Beratungsgruppe*, die sich aus anerkannten Sachverständigen der einschlägigen Interessenträger zusammensetzt, wozu u.a. KMUs, Betreiber wesentlicher Dienste, die IKT-Branche, die Datenschutzaufsicht sowie europäische Normungsorganisationen gehören. Die Beratungsgruppe unterstützt die *ENISA* bei der Aufgabendurchführung, die Cybersicherheitszertifizierung ausgenommen. Um die transnationale Vernetzung in der Cybersicherheit voranzutreiben und vor allem den Informationsaustausch noch weiter zu verbessern, wird ausgehend vom verabschiedeten Entwurf des Cybersecurity Act ein „Netz der nationalen Verbindungsbeamten" eingerichtet, das sich aus Vertretern der Mitgliedstaaten zusammensetzt.

Zertifizierungsrahmen und Cybersicherheitszertifizierung

Zentraler Regelungsansatz des Cybersecurity Act ist die nationalstaatenübergreifende Zertifizierung von Cybersicherheit. Grundlage hierfür sind europäische Schemata für die Cybersicherheitszertifizierung. Hierunter zu verstehen ist jeweils „ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, Diensten und Prozessen gelten". Das Europäische Cybersicherheitszertifikat wird definiert als ein „Dokument, in dem bescheinigt wird, dass ein bestimmter IKT-Prozess, ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde".

Ausarbeitung und Implementierung der Cybersicherheitsschemata

Zur Einrichtung eines europäischen Zertifizierungsrahmens für die Cybersicherheit wird ein Mechanismus etabliert, der die Bestimmung einzelner Schemata zur Cybersicherheitszertifizierung ermöglicht. Hierzu beauftragten die *EU-Kommission*, die auch den Arbeitsplan der Union für die Cybersicherheitszertifizierung festlegt, oder die noch einzurichtende Gruppe für die Cybersicherheitszertifizierung (ECCG) die *ENISA* mit der Ausarbeitung der entsprechenden Schemata, die sich auch auf einzelne Sektoren oder Branchen beziehen können. Die ECCG besteht aus Vertretern der nationalen Cybersicherheits-Zertifizierungsbehörden, auch soll die Beteiligung relevanter externer Stakeholder ermöglicht werden. Nach Beauftragung der *ENISA* erfolgt ein umfassender Konsultationsprozess von für das Cybersicherheitsschema relevanten Interessenträgern. Die Behörde ist bei Vorschlägen der ECCG allerdings nicht gezwungen, ein entsprechendes Schema auszuarbeiten, sondern kann dieses mit ordnungsgemäßer Begründung auch ablehnen. Bei jeder Erstellung eines Schemas soll die *ENISA* eine Ad-hoc-Arbeitsgruppe einrichten, zudem wird sie von der ECCG beraten. Unterstützend tritt ferner die „Gruppe der Interessenträger für die Cybersicherheitszertifizierung" hinzu, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt. Sie hat u.a. die Aufgabe, die *Kommission* in strategischen Fragen im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung zu beraten und soll dabei auch die Bezüge zur Normung herstellen.

Die final ausgearbeiteten Schemata treten mittels eines Durchführungsrechtsakts der *EU-Kommission* in Kraft. Daneben ist auch auf nationaler Ebene die Einführung von Zertifizierungsschemata möglich – sobald jedoch ein EU-Cybersicherheitsschema in Kraft tritt, verlieren entsprechende nationale Vorgaben ihre Gültigkeit, soweit sie in den europäisch regulierten Anwendungsbereich fallen.

Die angenommenen EU-Cybersicherheitsschemata werden von der *ENISA* mindestens alle fünf Jahre auf ihre Wirksamkeit hin überprüft. Die in diesem Zusammenhang relevanten Rückmeldungen von Interessenträgern fließen in die Bewertung ein. Eine Effizienzprüfung erfolgt separat alle zwei Jahre durch die *EU-Kommission*. In den bisherigen Entwürfen der Verordnung wie auch in der jetzt verabschiedeten Fassung ist die Zertifizierung als grundsätzlich freiwillige Maßnahme angedacht worden. Dennoch wird überprüft, ob für umgrenzte Bereiche die Notwendigkeit einer Pflichtzertifizierung besteht. Die vorrangige Priorität liegt dabei auf den wesentlichen Diensten (KRITIS) gemäß der RL (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Schutzniveaus von Netz- und Informationssystemen (NIS-RL), Anhang II.

Beibehaltung der bisherigen drei Anforderungsniveaus

Entsprechend den bisherigen Vorschlägen zum Cybersecurity Act wurden die drei Anforderungsniveaus „hoch", „mittel" und „niedrig" beibehalten. Die unterschiedlichen Anforderungsniveaus werden in Abhängigkeit vom jeweiligen Verwendungsrisiko bestimmt, wobei sich die zu Grunde liegenden, einzelnen Schemata auf spezifische IKT-Dienste und Produkte beziehen. Als Bestandteil des laufenden Arbeitsprogramms der *EU-Kommission* wird eine Liste relevanter IKT-Produkte und Dienste bis zu einem Jahr nach Inkrafttreten der Verordnung erstellt.

Eine Zertifizierung gemäß der Sicherheitsstufe „hoch" umfasst eine Prüfung der Abwehr hochmoderner Cyberangriffe mit umfangreichen Ressourcen, das Vorhandensein von IT-Sicherheitsfunktionen auf dem neuesten technischen Stand und den entsprechenden Nachweis durch Penetration-Testing. Für die Stufe „mittel" muss eine Abwehrfähigkeit im Hinblick auf bekannte Cyberrisiken durch Akteure mit begrenzten Ressourcen gegeben sein, eine Überprüfung auf öffentlich bekannte Schwachstellen erfolgen und die korrekte Funktion der Sicherheitsmaßnahmen durch Tests nachgewiesen werden. Für eine Zertifizierung gemäß den Anforderungen der Stufe „niedrig" muss mindestens die Minimierung grundlegender Risiken und die technische Dokumentation des Produkts oder Dienstes überprüft werden. Das Cybersicherheitsschema kann explizit die Möglichkeit des Herstellers zur Durchführung einer Selbstbewertung der Konformität vorsehen, wobei sich diese ausschließlich auf das Anforderungsniveau „niedrig" beziehen kann.

Mindestelemente eines EU-Cybersicherheits-Zertifizierungsschemas

Durch die Verordnung werden ferner die an die EU-Cybersicherheits-Zertifizierungsschemata anzulegenden inhaltlichen Anforderungen bestimmt, die der Entwicklung eines jeden Schemas zu Grunde liegen. So sind neben der jeweils vorgesehenen Vertrauenswürdigkeitsstufe u.a. Gegenstand, Ziele und Umfang des Schemas und die hiervon erfassten Produkte, Prozesse und Dienste zu benennen. Zudem wird eine eindeutige Beschreibung des Zwecks des Schemas und der Art und Weise, wie die ausgewählten Normen, Bewertungsmethoden und Vertrauenswürdigkeitsstufen mit den Erfordernissen der vorgesehenen Nutzer des Schemas in Einklang gebracht werden, benötigt. Die jeweiligen Schemata sollen überdies explizit auf die für die Bewertung maßgeblichen internationalen, europäischen oder nationalen Normen Bezug nehmen. Zu benennen sind ebenfalls die von den Antragstellern zur Überprüfung vorzulegenden Informationen und Nachweise sowie die Vorschriften zur Überwachung einer Einhaltung der mit der Zertifizierung verbundenen Anforderungen. Zudem sind für jedes Schema die Bedingungen zur Gewährung/Verlängerung des Zertifikats/der Konformitätserklärung, Vorgaben zu Meldung/Behandlung neuer Cybersicherheitslücken, Angaben zu vergleichbaren nationalen/internationalen Zertifizierungssystemen und inhaltliche Vorgaben zum ausgestellten Zertifikat/zur Konformitätserklärung zu bestimmen.

Anforderungen an Zertifizierungsstellen

Die künftige Zertifizierung nach dem EU-Cybersecurity Act erfolgt durch die nationalen Cybersicherheits-Zertifizierungsbehörden oder durch entsprechende Konformitätsbewertungsstellen. Für die Akkreditierung der Konformitätsbewertungsstellen zuständig ist die nationale Akkreditierungsstelle gem. VO (EG) 765/2008 (für Deutschland die *DAkkS*). Im Falle privater Konformitätsbewertungsstellen gelten umfassende Anforderungen im Hinblick auf deren Autonomie, Fachkunde und Transparenz. Die Akkre-

ditierung der Konformitätsbewertungsstellen kann für die Höchstdauer von fünf Jahren erteilt werden, wobei bei weiterer Erfüllung der Anforderungen eine Verlängerung möglich ist. Für jedes angenommene EU-Schema zur Cybersicherheitszertifizierung erfolgt eine Notifizierung der entsprechenden Konformitätsbewertungsstellen durch die nationalen Cybersicherheits-Zertifizierungsbehörden gegenüber der *EU-Kommission*, woraufhin diese im Amtsblatt der EU die Liste der notifizierten Konformitätsbewertungsstellen veröffentlicht. Zur zusätzlichen Qualitätssicherung ist ferner ein Peer-Review der nationalen Cybersicherheits-Zertifizierungsbehörde im mindestens fünfjährigen Turnus vorgesehen.

■ Vgl. auch *Kipker/Scholz*, MMR-Aktuell 2018, 410979; *Kipker/Mueller,* MMR-Aktuell 2019, 414291; *Kipker*, MMR-Aktuell 2017, 395945; *ders.,* MMR-Aktuell 2017, 394677 und *ders.*, MMR 2017, 143.

Dr. Dennis-Kenji Kipker
ist Geschäftsführer der CERTAVO GmbH – international compliance management, wissenschaftlicher Geschäftsführer des IGMR an der Universität Bremen, Legal Advisor für den VDE e.V. – Abteilung CERT@VDE – in Frankfurt/M. und Mitglied des Vorstandes der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.

Dario Scholz
ist studentischer Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen.