



## **Cybersicherheit: Kommission schlägt Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit vor**

*Trilogverhandlungen zum Cybersecurity-Act haben begonnen*

Die Europäische Kommission hat am 12.09.2018 einen Verordnungsvorschlag (KOM (2018) 630 final) zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren vorgelegt.

### **Hintergrund**

Angesichts der raschen technologischen Entwicklungen und der zunehmenden Bedrohungen im Cybersicherheitsbereich sieht die Kommission die Notwendigkeit, Fachwissen über Fragen der Cybersicherheit auf EU-Ebene zu bündeln. Grund ist die unzureichende Zusammenarbeit zwischen den verschiedenen Akteuren auf dem Markt sowie zwischen den Mitgliedstaaten. Ziel des Vorschlags ist, die Kapazitäten der EU im Bereich Cybersicherheit auszubauen und die Wettbewerbsfähigkeit der europäischen Cybersicherheitsbranche zu stärken.

Der Vorschlag umfasst drei Elemente: das Europäische Kompetenzzentrum (1), das Netzwerk nationaler Koordinierungszentren (2) und die Kompetenzgemeinschaft (3). Über die Kosten und Finanzierung (4) des Kompetenzzentrums ist noch nicht vollständig entschieden worden.

### **Europäisches Kompetenzzentrum**

Der Vorschlag sieht vor, ein Europäisches Kompetenzzentrum (Art. 4, 5, 10 ff., 31 f.) mit Sitz in Brüssel (Art. 1 Abs. 3) zu gründen. Die Aufgaben sollen u.a. umfassen:

- Erleichterung und Unterstützung der Koordinierung der Arbeiten des Netzes nationaler Koordinierungszentren;
- Verbesserung der Kapazitäten, des Wissens und der Infrastruktur im Bereich der Cybersicherheit, die der Industrie, dem öffentlichen Sektor und der Forschung zur Verfügung stehen;
- Durchführung der betreffenden Teile der Programme „Digitales Europa“ und „Horizont Europa“;

- Beitrag zur umfassenden Einführung modernster Cybersicherheitsprodukte und -lösungen;
- Beitrag zur Stärkung der Cybersicherheitsforschung und -entwicklung.

Das Kompetenzzentrum soll sich zukünftig aus einem Verwaltungsrat, einem Exekutivdirektor und einem wissenschaftlich-technischen Beirat zusammensetzen (Art. 11 Abs. 2).

Das wichtigste Entscheidungsgremium ist der Verwaltungsrat, in dem zwar alle Mitgliedstaaten vertreten sind, aber nur jene Mitgliedstaaten, die sich auch finanziell beteiligen, ein Stimmrecht haben. Der Verwaltungsrat besteht aus je einem Vertreter pro Mitgliedstaat und fünf Kommissionsvertretern, die im Namen der Europäischen Union handeln. Er trägt die Gesamtverantwortung für die strategische Ausrichtung und die Geschäfte des Kompetenzzentrums und beaufsichtigt die Durchführung seiner Tätigkeiten. Der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) soll ein ständiger Beobachter werden. Die Union und die beteiligten Mitgliedstaaten verfügen über jeweils 50 % der Stimmrechte. Die Beschlussfassung erfolgt mit einer Mehrheit von mindestens 75 % aller Stimmen (Art. 15).

Der Exekutivdirektor wird vom Verwaltungsrat für vier Jahre aus einer Liste von Bewerbern ernannt, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorschlägt (Art. 16). Er soll für den Tagesbetrieb und die Geschäftsführung des Kompetenzzentrums verantwortlich sein und soll dessen gesetzlicher Vertreter werden (Art. 17 Abs. 1).

Der wissenschaftlich-technische Beirat besteht aus höchstens 16 Mitgliedern, welche vom Verwaltungsrat aus dem Kreis der Vertreter der Einrichtungen in der Kompetenzgemeinschaft für Cybersicherheit für eine Amtszeit von drei Jahren ernannt werden. Der Beirat berät das



Kompetenzzentrum bei der Durchführung seiner Tätigkeiten (Art. 20).

## Netzwerk nationaler Koordinierungszentren

Jeder Mitgliedstaat soll ein nationales Koordinierungszentrum benennen, das dem Netzwerk angehört. Aufgabe der Koordinierungszentren ist die Koordination des Austausches über Cybersicherheits-Fachwissen zwischen dem privaten, öffentlichen und wissenschaftlichen Sektor. Dabei sollen die Zentren als Kontaktstelle auf nationaler Ebene fungieren und das Kompetenzzentrum bei der Erreichung seiner Ziele unterstützen.

## Kompetenzgemeinschaft

Die Kompetenzgemeinschaft besteht aus einer Gruppe von Interessenträgern im Bereich Cybersicherheit aus der Wissenschaft sowie aus dem privaten und dem öffentlichen Sektor, einschließlich Zivil- und Militärbehörden. Sie bringt damit die wichtigsten Interessenträger (z.B. Forschungseinrichtungen und Verbände) im Hinblick auf die technischen und industriellen Kapazitäten in der Union zusammen. Fachkompetenz in den Bereichen Forschung, industrielle Entwicklung, Schulung und Bildung sollen dabei erfasst und nachgewiesen werden. Nur Einrichtungen, die in der Union niedergelassen sind, können als Mitglieder der Kompetenzgemeinschaft durch das Kompetenzzentrum akkreditiert werden

In Zusammenarbeit mit der Kompetenzgemeinschaft und dem Netz nationaler Koordinierungszentren soll das Europäische Kompetenzzentrum für Cybersicherheit die wichtigste Durchführungsstelle für die Verwendung von EU-Finanzmitteln werden.

## Finanzierung

Das Kompetenzzentrum soll in Form einer europäischen Partnerschaft eingerichtet werden, bestehend aus gemeinsamen Investitionen durch die Union, die Mitgliedstaaten und/oder die Industrie. Deshalb sieht der Vorschlag vor, dass die Mitgliedstaaten einen angemessenen Beitrag zu den Maßnahmen des Kompetenzzentrums und des Netzes beisteuern müssen. Laut Artikel 21 sollen rund 2 Mrd. Euro aus dem Programm „Horizont Europa“ zur Deckung der

Verwaltungs- und Betriebskosten verwendet werden. Die Mitgliedstaaten sollen zudem einen eigenen finanziellen Beitrag leisten, der mindestens derselben Höhe entspricht. Ein Finanz- und ein Tätigkeitsbericht soll jährlich vorgestellt werden.

## Aktueller Stand der Verhandlungen

Federführend im Europäischen Parlament ist der Ausschuss für Industrie, Forschung und Energie (ITRE), dem dieser Vorschlag am 01.10.2018 übertragen wurde. Ein Berichterstatter wurde offiziell noch nicht ernannt. Gleichmaßen im Anfangsstadium befindet sich der Vorschlag im Rat.

## Verordnungsvorschlag „Cybersecurity-Act“

Neben den neuen Regeln zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit wurden zuvor bereits andere Maßnahmen zur Erhöhung der Abwehrfähigkeit und zur Verbesserung ihrer Abwehrbereitschaft im Bereich der Cybersicherheit durch die EU getroffen und vorgeschlagen. Der Verordnungsvorschlag zur Cybersicherheit (sog. Cybersecurity-Act, KOM (2017) 477) aus dem Jahr 2017 befindet sich zurzeit in Trilogverhandlungen.

Der Cybersecurity-Act sieht vor, die bereits seit 2005 bestehende Europäische Agentur ENISA zur Europäischen Cybersicherheitsagentur mit permanentem Mandat und umfangreicheren Zuständigkeiten umzugestalten und damit zur zentralen Stelle für die Entwicklung der EU-Politik im Bereich Netz- und Informationssicherheit zu machen. Ihr sollen neue Aufgaben zur Unterstützung der Mitgliedstaaten, der europäischen Institutionen und sonstiger Interessenträger in Fragen der Cybersicherheit übertragen sowie ihre finanziellen und personellen Mittel wesentlich erhöht werden. Des Weiteren sollen regelmäßige EU-weite Cybersicherheitsübungen durch sie organisiert werden. Um den Informationsaustausch zwischen ENISA und den Mitgliedstaaten zu vereinfachen, ist beabsichtigt ein Netz nationaler Verbindungsbeamten einzusetzen. Zudem sieht der Verordnungsvorschlag die Einführung eines EU-weiten Rahmens für die Zertifizierung für IT-Produkte und -dienste vor. Die bisher bestehenden verschiedenen nationalen Sicherheitszertifizierungssysteme

# Die Landesvertretung Nordrhein-Westfalen in Brüssel informiert



mit jeweils eigenen Prüfverfahren und Anforderungen haben zu einer starken Fragmentierung des Binnenmarktes beigetragen und stellen Hindernisse im Digitalen Binnenmarkt dar. Mit EU-weit geltenden Sicherheitszertifikaten soll das Vertrauen der Käufer in die Sicherheitseigenschaften eines IT-Produkts gestärkt und der Handel für Unternehmen erleichtert werden.

Nach der allgemeinen Ausrichtung des Rates ist die Einrichtung einer "European Cybersecurity Certification Group" aus Repräsentanten der für die Cyber-Sicherheitszertifizierung zuständigen nationalstaatlichen Behörden geplant. Diese soll auch in Zusammenarbeit mit sonstigen Stakeholdern wie Industrie- und Verbraucherverbänden ENISA bei der Harmonisierung bzw. Neuentwicklung von Zertifizierungsschemata unterstützen. Dadurch soll den Mitgliedstaaten – und nicht alleine ENISA - weiterhin eine wichtige Rolle bei der Entwicklung der Cyber-Sicherheitszertifizierung zukommen.

In den bisherigen Trilogverhandlungen, die nach der Sommerpause begonnen haben, wurden politische und technische Probleme behandelt. Wichtige Elemente der Diskussion waren die Vorbereitung und Annahme eines europäischen Systems für die Cybersicherheitszertifizierung in Verbindung mit der Zertifizierungsgruppe der Mitgliedstaaten, die Zertifizierungsgruppe der Interessenträger, das fortlaufende Arbeitsprogramm für europäische Cybersicherheitszertifizierungssysteme und die ENISA-Aufgaben in Bezug auf den Markt, Cybersicherheitszertifizierung und Standardisierung. Dabei wurde der Zertifizierungsprozess in verschiedene Phasen unterteilt: Vorschlag, Antrag, Vorbereitung, Übermittlung und Annahme. Im Übrigen verteidigte der Österreichische Vorsitz die allgemeine Ausrichtung des Rates und seinen Standpunkt, ersuchte jedoch die Delegationen um Orientierungshilfe in Bezug auf die neuen Elemente des Textes seitens des Europäischen Parlamentes, die noch nicht mit den Mitgliedstaaten erörtert wurden.

Da im Grundsatz Einigung zwischen dem Rat und dem Parlament besteht, stehen die Chancen gut, dass die Verordnung noch vor

Ende der Legislatur und den Neuwahlen 2019 beschlossen wird.

---

Weiterführende Informationen:

Gemeinsame Erklärung von Kommissionspräsident Jean-Claude Juncker, EU-Ratspräsident Donald Tusk und der Vizepräsidentin Federica Mogherin zu Cyberangriffen:

[https://ec.europa.eu/germany/news/20181004-gemeinsame-erklaerung-zu-cyberangriffen\\_de](https://ec.europa.eu/germany/news/20181004-gemeinsame-erklaerung-zu-cyberangriffen_de)

Vorschlag der Verordnung:

<https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-630-F1-DE-MAIN-PART-1.PDF>