CYBERSICHERHEIT – TEIL 2: ZERTIFIZIERUNG

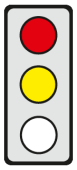
Centrum für Europäische Politik

cep**Analyse** Nr. 16/2018

KERNPUNKTE

Ziel der Verordnung: Die Kommission will durch ein europäisches Zertifizierungssystem für Cybersicherheit das Vertrauen in Produkte und Dienste der Informations- und Kommunikationstechnik (IKT) stärken.

Betroffene: Alle Verbraucher und Unternehmen, insbesondere der IKT-Branche, EU-Cybersicherheitsagentur ENISA, nationale Aufsichtsbehörden, Konformitätsbewertungs- und Akkreditierungsstellen.



Pro: (1) EU-weite Regeln für die Cybersicherheitszertifizierung können den Markt für cybersichere IKT-Produkte und -Dienste beleben.

Contra: (1) Es ist fraglich, ob Kommission und ENISA über das Wissen verfügen, für welche IKT-Produkte und -Dienste ein Europäisches System für die Cybersicherheitszertifizierung (ESCZ) sinnvoll erscheint.

(2) Die Mitgliedstaaten sollten bei der Erarbeitung von ESCZ zwingend eingebunden werden.

(3) Der EU-Gesetzgeber darf keine Cybersicherheitsregelungen erlassen, die die nationale Sicherheit der Mitgliedstaaten berühren. Es sollte daher klargestellt werden, dass die Mitgliedstaaten insoweit ein höheres Schutzniveau vorsehen und ein bestehendes nationales System für die Cybersicherheitszertifizierung (NSCZ) aufrechterhalten dürfen.

Die wichtigsten Passagen im Text sind durch einen Seitenstrich gekennzeichnet.

INHALT

Titel

Vorschlag COM(2017) 477 vom 4. Oktober 2017 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**

Kurzdarstellung

- **Hintergrund und Ziele**
  - Laut Kommission führt die zunehmende Digitalisierung und Vernetzung vieler gesellschaftlicher Bereiche zu einem Anstieg von Cybersicherheitsrisiken und -angriffen (Erwägungsgrund 2 und 3).
  - Die Kommission will angesichts dieser Herausforderungen insbesondere (Erwägungsgrund 5)
    - die Fähigkeiten der Mitgliedstaaten und Unternehmen bei der Abwehr von Cyberangriffen stärken,
    - die Zusammenarbeit zwischen den Mitgliedstaaten und den EU-Einrichtungen verbessern und
    - das Vertrauen in den digitalen Binnenmarkt durch mehr Transparenz über das Niveau der Sicherheit von Informations- und Kommunikationstechnik (IKT) stärken.
  - Dies soll im Wesentlichen erreicht werden durch (Begründung S. 4 und 7, Erwägungsgrund 11)
    - die Reform der EU-Cybersicherheitsagentur „ENISA“ (s. cep**Analyse**) und
    - die Zertifizierung der Cybersicherheit von IKT (diese cep**Analyse**).

- **Status quo der Zertifizierung der Cybersicherheit in der EU**
  - Derzeit basiert die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (IKT) in der EU auf verschiedenen Abkommen und auf Initiativen einzelner Mitgliedstaaten (Begründung S. 10, 11:
    - Ein internationales Abkommen regelt die Anerkennung der „allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie“ [Common Criteria (CC) for IT Security Evaluation], das 13 Mitgliedstaaten unterzeichnet haben; die CC sind eine internationale Norm zur Evaluierung der IT-Sicherheit.
    - Das „SOG-IS“-Abkommen, das die Behörden von zwölf EU-Staaten und Norwegen geschlossen haben, regelt für eine begrenzte Zahl von Produkten wie digitale Signaturen die gegenseitige Anerkennung von Zertifikaten.
    - Großbritannien, Frankreich und Deutschland haben nationale Initiativen zur IKT-Zertifizierung ergriffen.

- **Künftiges Regelwerk zur Zertifizierung der Cybersicherheit in der EU**
  - Laut Kommission können die verschiedenen Abkommen und Initiativen zu Marktfragmentierung führen. Unternehmen müssen häufig mehrere Zertifizierungsverfahren durchlaufen, was ihre Kosten und den Verwaltungsaufwand erhöht. (Begründung S. 11)
  - Die Kommission will mit der Verordnung einen „europäischen Rahmen“ für die Zertifizierung der Cybersicherheit von IKT-Produkten und -Diensten etablieren (Begründung S. 11, 12, Erwägungsgrund 52 und 53).

Autoren: Philipp Eckhardt und Dr. Anja Hoffmann, LL.M. Eur. | eckhardt@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-107 | www.cep.eu

– Kernelement des Rahmens sind einzelne von der ENISA auszuarbeitende „Europäische Systeme für die Cybersicherheitszertifizierung“ (im Folgenden: ESCZ) für spezifische IKT-Produkte und -Dienste oder Gruppen davon. Die ausgearbeiteten ESCZ stellen das jeweilige Regelwerk zur Zertifizierung der jeweiligen IKT-Produkte und -Dienste bzw. Gruppen dar. (Begründung S. 11, 12, Erwägungsgrund 52 und 53, Art. 44 Abs. 1)
– Der Begriff „IKT-Produkte und -Dienste“ umfasst auch Prozesse und Systeme sowie Kombinationen dieser Elemente (Art. 2 Ziff. 11, Erwägungsgrund 47).
– Die ENISA konsultiert vor der Ausarbeitung eines jeden ESCZ alle „relevanten“ Interessenträger und die neu einzusetzende Gruppe für die Cybersicherheitszertifizierung (nachfolgend: Gruppe), die sich aus den Vertretern der nationalen Zertifizierungsbehörden unter Vorsitz der Kommission zusammensetzt (Art. 44 Abs. 2, Art. 53).
– Die Kommission beauftragt die ENISA mit der Ausarbeitung eines ESCZ. „Die Mitgliedstaaten“ oder die Gruppe können der Kommission vorschlagen, die ENISA mit der Ausarbeitung zu beauftragen. (Art. 44 Abs. 1)
– Die Kommission verabschiedet die ausgearbeiteten ESCZ durch Durchführungsrechtsakte (Art. 44 Abs. 3 und 4).

► **Sicherheitsziele, Mindestinhalte und Vertrauenswürdigkeitsstufen der verschiedenen ESCZ**
– Die Verordnung legt die „Sicherheitsziele“ (Art. 45) und die „Mindestinhalte“ (Art. 47 Abs. 1) fest.
– Für alle ESCZ gelten folgende „Sicherheitsziele“ (Art. 45):
  - Daten sind u.a. geschützt vor zufälliger oder unbefugter Speicherung, Verarbeitung oder Preisgabe,
  - nur befugte Personen, Programme und Maschinen haben Zugriff auf Daten, Dienste und Funktionen der IKT-Produkte und -Dienste,
  - IKT-Produkte und -Dienste werden mit aktueller Software ohne bekannte Sicherheitslücken bereitgestellt.
– Bei der Ausarbeitung eines spezifischen ESCZ müssen u.a. folgende „Mindestinhalte“ festgelegt werden (Art. 47 Abs. 1, Begründung S. 12 und 14):
  - die Cybersicherheitsanforderungen, z.B. durch Bezugnahme auf europäische oder internationale Normen,
  - die Art(en) und Kategorie(n) der IKT-Produkte und -Dienste, die von dem ESCZ erfasst sind, und
  - die Vertrauenswürdigkeitsstufen, also Sicherheitsniveaus, die durch das ESCZ gewährleistet werden sollen.
– ESCZ-zertifizierte IKT-Produkte und -Dienste können in drei Vertrauenswürdigkeitsstufen – niedrig, mittel, hoch – eingestuft werden (Art. 46).

► **Cybersicherheitszertifizierung auf Grundlage eines ESCZ**
– Natürliche und juristische Personen, die ihre IKT-Produkte oder -Dienste auf der Grundlage eines spezifischen ESCZ zertifizieren lassen wollen, müssen die Zertifizierung bei einer „Konformitätsbewertungsstelle“ beantragen und dieser die notwendigen Informationen zur Verfügung stellen (Art. 48 Abs. 5, Erwägungsgrund 58).
– Die Konformitätsbewertungsstelle bewertet, ob die IKT-Produkte oder -Dienste die Anforderungen des jeweiligen ESCZ erfüllen und stellt die Cybersicherheitszertifikate aus (Art. 2 Ziff. 14 und 15, Art. 48 Abs. 3).
– Von den Mitgliedstaaten benannte „nationale Akkreditierungsstellen“ erteilen den Konformitätsbewertungsstellen die Akkreditierung für ihre Tätigkeit. Die Akkreditierungen werden für fünf Jahre erteilt, können aber verlängert werden. (Art. 51 i.V.m. Art. 4 Abs. 1 der Verordnung (EG) Nr. 765/2008)
– Für ausgestellte Zertifikate gilt die „Vermutung“ der Konformität mit den Anforderungen des spezifischen ESCZ (Art. 48 Abs. 1). Die Zertifikate „garantieren“ die Erfüllung der Anforderungen an die Cybersicherheit jedoch nicht (Erwägungsgrund 47).
– Zertifikate werden für maximal drei Jahre erteilt, können aber verlängert werden (Art. 48 Abs. 6).
– Ausgestelle Zertifikate müssen in allen Mitgliedstaaten anerkannt werden (Art. 48 Abs. 7).
– Die Zertifizierung ist freiwillig, sofern das EU-Recht nichts anderes festlegt (Art. 48 Abs. 2).

► **Rolle der Mitgliedstaaten und der nationalen Aufsichtsbehörden**
– Jeder Mitgliedstaat benennt eine „nationale Aufsichtsbehörde für die Zertifizierung“, die u.a. (Art. 50 Abs. 1, 6)
  – die von den Konformitätsbewertungsstellen ausgestellten Zertifikate überprüft,
  – die Tätigkeiten der Konformitätsbewertungsstellen beaufsichtigt und
  – mit anderen nationalen Aufsichtsbehörden und öffentlichen Stellen zusammenarbeitet.
– Die nationalen Aufsichtsbehörden müssen der Kommission für jedes spezifische ESCZ eine zuständige Konformitätsbewertungsstelle benennen (Art. 52).
– Die Mitgliedstaaten behalten „unberührt“ von den Aufgaben der ENISA ihre Zuständigkeiten für Cybersicherheit. Dies gilt „in jedem Fall“ für Tätigkeiten in Zusammenhang mit der nationalen und öffentlichen Sicherheit, der Landesverteidigung und für strafrechtliche Belange. (Art. 3 Abs. 3)

► **Nationale und industrielle Cybersicherheitszertifizierungssysteme**
– Umfasst ein bestehendes nationales System für die Cybersicherheitszertifizierung („NSCZ“) IKT-Produkte und -Dienste, die auch Gegenstand eines ESCZ sind, ist das NSCZ ab dem Zeitpunkt unwirksam, den die Kommission dafür in ihrem Durchführungsrechtsakt zu dem ESCZ festgelegt hat (Art. 49 Abs. 1).
– Die Mitgliedstaaten dürfen keine neuen NSCZ für IKT-Produkte und -Dienste einführen, die unter ein ESCZ fallen. Unter den NSCZ ausgestellte Zertifikate gelten bis zum Ende ihrer Geltungsdauer fort. (Art. 49 Abs.2,3)
– Private Zertifizierungssysteme u.a. der Industrie sind nicht Gegenstand der Verordnung. Verantwortliche Stellen können ihre Systeme der Kommission aber zur Genehmigung als ESCZ vorschlagen. (Erwägungsgrund 53)

Subsidiaritätsbegründung der Kommission

Die über Landesgrenzen hinweg bestehenden Abhängigkeiten zwischen Netz- und Informationssystemen sind groß. Wegen dieser Abhängigkeiten sind einzelne Akteure Cybersicherheitsbedrohungen nicht allein gewachsen und können diese häufig nicht isoliert bewältigen. Daher sind EU-Maßnahmen notwendig.

Politischer Kontext

Die Kommission legte 2016 eine Mitteilung zur Stärkung der Abwehrfähigkeit Europas bei der Cybersicherheit vor [COM(2016) 410], in der sie Rahmenregeln für die Zertifizierung der Sicherheit von IKT-Produkten und -Diensten erwog. Auch der Rat forderte die Kommission 2016 auf, tätig zu werden.

Stand der Gesetzgebung

04.10.17	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien (federführend)
Ausschüsse des Europäischen Parlaments:	Industrie, Technologie und Energie (federführend), Berichterstatterin: Angelika Niebler (EVP-Fraktion, Deutschland)
Bundesministerien:	Bundesministerium für Inneres (federführend)
Ausschüsse des Deutschen Bundestags:	Inneres (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt);
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Die Investitionen in Cybersicherheit sind aus zwei Gründen gering. Erstens sind die meisten Verbraucher nicht in der Lage einzuschätzen, wie „cybersicher" bestimmte Produkte und Dienste tatsächlich sind. Ihre Zahlungsbereitschaft für vermeintlich sichere Produkte und Dienste ist daher gering. In der Folge halten sich auch die Anbieter mit Investitionen zurück. Als Ergebnis dieser Informationsasymmetrie ist das Niveau der Cybersicherheit niedrig („Market for lemons"). Zweitens verzichten viele Verbraucher auf Investitionen in die Cybersicherheit, da der individuelle Schaden bei einem – als unwahrscheinlich eingeschätzten – Sicherheitsvorfall gering erscheint. Sie preisen bei dieser Entscheidung jedoch nicht die negativen Folgen eines Sicherheitsvorfalls bei sich für Dritte mit ein (Nichtinternalisierung externer Effekte) und profitieren von den Investitionen Dritter (Trittbrettfahrerverhalten).

EU-weite Regeln für die Cybersicherheitszertifizierung können die Problematik der Informationsasymmetrien lindern und **den Markt für cybersichere IKT-Produkte und -Dienste beleben.** Voraussetzung dafür ist, dass die Verbraucher die Zertifizierung als glaubwürdig ansehen. Das Problem der Nichtinternalisierung externer Effekte und das Trittbrettfahrer-Problem bestehen allerdings weiterhin. Tendenziell führen Zertifizierungen auch zu einer Verteuerung der Produkte und Dienste. Dies wirkt den positiven Effekten entgegen.

Die geplanten **Systeme für die Cybersicherheitszertifizierung – ESCZ – führen zu einem erheblichen Machtzuwachs der ENISA und der EU-Kommission.** Nur diese Behörden entscheiden letztlich über die Einführung und Gestaltung von ESCZ. **Es ist** jedoch **fraglich, ob Kommission und ENISA über das** nötige **Wissen verfügen, für welche IKT-Produkte und -Dienste ein ESCZ sinnvoll erscheint und wie dieses ausgestaltet sein sollte**. Insbesondere bei der ENISA ist ferner fraglich, ob sie über das nötige Personal für die Ausarbeitung der ESCZ verfügt (s. dazu cep**Analyse** zur ENISA-Reform). Auch fehlen eine präzise Abgrenzung, was als „IKT-Produkte und -Dienste" unter die Verordnung fällt – etwa auch Prozesse zu deren Entwicklung –, und inwiefern ESCZ Anwendungsfälle erfassen, die die nationale Sicherheit der Mitgliedstaaten betreffen.

Dass Unternehmen künftig ihre **IKT-Produkte und -Dienste in einem Mitgliedstaat zertifizieren lassen können und die Zertifikate dann EU-weite Anerkennung erlangen** („One stop shop-System")**, senkt ihre Kosten, birgt aber die Gefahr, dass sie sich** für die Zertifizierung **den Mitgliedstaat aussuchen, in dem sie die Zertifizierung mit dem geringsten Aufwand erhalten.** Dies birgt das Risiko einer laxen Prüfung von Cybersicherheitsanforderungen und im Ergebnis weniger sicherer IKT-Produkte und -Dienste. Dem könnte ein Kontrollverfahren unter den nationalen Aufsichtsbehörden oder durch die ENISA abhelfen.

Sachgerecht ist, dass die Zertifizierungen selbst grundsätzlich freiwillig bleiben. Nur in hochsensiblen Anwendungsgebieten kann eine gesetzliche Pflicht zur Zertifizierung vertretbar sein. In Bereichen, bei denen geringe Risiken für Dritte hinsichtlich der Cybersicherheit bestehen, wirken Zertifizierungen als unnötige und teure Markteintrittsbarriere und verhindern letztlich Innovationen.

Juristische Bewertung

Kompetenz

Die Regelungen zur Zertifizierung sind von der Binnenmarktkompetenz (Art. 114 AEUV) gedeckt. Zwar erfolgt die Angleichung nicht allein durch die Verordnung, weil die Einzelheiten erst in den ESCZ geregelt werden. Auf Art. 114 können aber auch Rechtsakte gestützt werden, die lediglich die Kompetenz zur Angleichung mittels Durchführungsmaßnahmen auf die Kommission übertragen (EuGH, Rs. C-66/04, Rn. 51). Wegen der technischen Komplexität der Materie darf **der EU-Gesetzgeber** auch die ENISA als Agentur zur koordinierten Harmonisierung der ESCZ heranziehen (vgl. dazu EuGH, Rs. C-217/04, Rn. 44 ff). Er **darf** jedoch **keine Cybersicherheitsregelungen erlassen, die die nationale Sicherheit der Mitgliedstaaten berühren.** Hierfür haben die Mitgliedstaaten die alleinige Verantwortung (Art. 4 Abs. 2 S. 3 EUV). **Es sollte daher klargestellt werden, dass die Mitgliedstaaten insoweit ein höheres Schutzniveau vorsehen und** ggf. (ergänzende) **NSCZ aufrechterhalten dürfen.**

Subsidiarität

Der EU-Rahmen für die Zertifizierung ist mit dem Subsidiaritätsprinzip vereinbar. Zwar existiert mit dem „SOG-IS MRA“ zwischen 12 Mitgliedstaaten bereits ein Anerkennungsabkommen für nationale Zertifikate. Dieses wird in der Praxis aber nur für die Zertifizierung von Produkten genutzt, die eine hohe Vertrauenswürdigkeitsstufe erfordern. Eine umfassende Harmonisierung auch für Produkte mit niedrigerer Vertrauenswürdigkeit oder für IKT-Dienste kann nur durch einen gesonderten EU-Rahmen erreicht werden.

Grundsätzlich ist die Durchführung des EU-Rechts Aufgabe der Mitgliedstaaten. Der EU-Gesetzgeber darf aber die Kommission ermächtigen, ESCZ per Durchführungsbeschluss festzulegen, wenn es „einheitlicher Bedingungen für die Durchführung bedarf“ (Art. 291 Abs. 2 AEUV). **Die Kommission sollte die ESCZ** aber **statt in Durchführungsrechtsakten** (Art. 291 AEUV) **in delegierten Rechtsakten** (Art. 290 AEUV) **festlegen**, da sie die Verordnung durch die ESCZ ergänzt, aber nicht i.e.S. „durchführt“. Dies würde auch deren demokratische Legitimation stärken.

Dem steht nicht entgegen, dass wichtige Details der Zertifizierung wie Produkte und technische Anforderungen erst in den ESCZ festgelegt werden. Zwar ist der EU-Gesetzgeber verpflichtet, alle wesentlichen Aspekte selbst zu regeln. „Wesentlich“ sind aber nur Vorschriften, durch die die grundsätzliche Ausrichtung der EU-Politik umgesetzt wird (EuGH Rs. C-240/90, Rn. 37). Die grundsätzliche Ausrichtung der Zertifizierung – Ziele, Elemente und Wirkungen der ESCZ – wird jedoch durch die Verordnung festgelegt.

Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Die Verordnung greift in die Befugnis der Mitgliedstaaten ein, die Cybersicherheit in ihrem Staat zu regeln. Die Unwirksamkeit von NSCZ und die Verpflichtung, alle ESCZ-Zertifikate anzuerkennen, können zu einer Absenkung des Schutzniveaus in den Mitgliedstaaten führen. **Um ein hohes technisches Sicherheitsniveau zu erzielen** (Art. 114 Abs. 3 AEUV) **und ein Scheitern von ESCZ** im Komitologieverfahren (s. Erwägungsgrund 65) bzw. Einwände gegen den delegierten Rechtsakt **zu vermeiden**, **sollten die Mitgliedstaaten** und die Wirtschaft **bei deren Erarbeitung zwingend eingebunden** und nicht lediglich „konsultiert“ **werden**. **Zudem sollte** ausdrücklich **klargestellt werden, dass die Mitgliedstaaten die Verwendung von IKT-Produkten und -Diensten an strengere** (nationale) **Voraussetzungen knüpfen dürfen**, **soweit der Schutz wichtiger** – auch über den engen Bereich der „nationalen Sicherheit“ hinausgehender – **nationaler Interessen** wie der öffentlichen Sicherheit, der Landesverteidigung oder des Strafrechts (Art. 3 Abs. 3) **dies erfordert**.

Auswirkungen auf das deutsche Recht

Insbesondere müssen das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie die BSI-Zertifizierungs- und Anerkennungsverordnung geändert werden.

Zusammenfassung der Bewertung

EU-weite Regeln für die Cybersicherheitszertifizierung können den Markt für cybersichere IKT-Produkte und -Dienste beleben. Es ist fraglich, ob Kommission und ENISA über das Wissen verfügen, für welche IKT-Produkte und -Dienste ein ESCZ sinnvoll erscheint. Der EU-Gesetzgeber darf keine Cybersicherheitsregelungen erlassen, die die nationale Sicherheit der Mitgliedstaaten berühren. Es sollte daher klargestellt werden, dass die Mitgliedstaaten insoweit ein höheres Schutzniveau vorsehen und NSCZ aufrechterhalten dürfen. Die Kommission sollte die ESCZ statt in Durchführungsrechtsakten in delegierten Rechtsakten festlegen. Um ein hohes technisches Sicherheitsniveau zu erzielen und ein Scheitern von ESCZ zu vermeiden, sollten die Mitgliedstaaten bei deren Erarbeitung zwingend eingebunden werden. Zudem sollte klargestellt werden, dass die Mitgliedstaaten die Verwendung von IKT-Produkten und -Diensten an strengere Voraussetzungen knüpfen dürfen, soweit der Schutz wichtiger nationaler Interessen dies erfordert.