
Deutsche Industrie- und Handelskammer

Stellungnahme

Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2, CSA 2)

Mit dem am 20. Januar 2026 vorgelegten Vorschlag für einen neuen Cybersecurity Act verfolgt die Europäische Kommission das Ziel, bestehende Cybersicherheitsvorgaben besser aufeinander abzustimmen, die Umsetzung bestehender Regelwerke wie der NIS-2-Richtlinie zu erleichtern und die Fragmentierung des europäischen Binnenmarktes zu reduzieren. Die Rolle der Europäischen Agentur für Cybersicherheit (ENISA) soll gestärkt, der europäische Zertifizierungsrahmen weiterentwickelt und die Sicherheit von IKT-Lieferketten verbessert werden.

Die Deutsche Industrie- und Handelskammer (DIHK) unterstützt das Ziel eines hohen und einheitlichen Cybersicherheitsniveaus in Europa. Cybersicherheit und Wettbewerbsfähigkeit müssen dabei gemeinsam gedacht werden. Regulierung sollte Unternehmen bei der Erfüllung ihrer Pflichten unterstützen, Bürokratie abbauen und zu einer weiteren Harmonisierung des Binnenmarktes beitragen. Maßnahmen zur Absicherung von Lieferketten dürfen dabei nicht zu Investitionshemmnissen, Versorgungslücken oder neuen Wettbewerbsnachteilen für europäische Unternehmen führen. Wir bedanken uns für die Gelegenheit zur Stellungnahme.

Das Wichtigste in Kürze

Die europäische Wirtschaft ist auf ein hohes Cybersicherheitsniveau angewiesen. Unternehmen stehen bereits heute vor einer Vielzahl regulatorischer Anforderungen aus NIS-2, Cyber Resilience Act, Datenschutzrecht und weiteren branchenspezifischen Rechtsakten wie der Medical Device Regulation (MDR). Der CSA 2 kann einen wichtigen Beitrag zur Stärkung des europäischen Binnenmarktes leisten, wenn er bestehende Regelungen konsequent harmonisiert, Bürokratie abbaut und Cybersicherheit mit Wettbewerbsfähigkeit verbindet. Dabei wird es auch auf eine harmonisierte Umsetzung in den Mitgliedstaaten ankommen, um Wettbewerbsverzerrungen zu vermeiden.

Damit der CSA 2 sein Potenzial zur Stärkung von Cybersicherheit und Wettbewerbsfähigkeit voll entfalten kann, sind aus Sicht der Wirtschaft insbesondere die folgenden Punkte zu berücksichtigen:

- Vermeidung zusätzlicher und paralleler Meldepflichten

Mehrfache Meldewege für denselben Sicherheitsvorfall verursachen erheblichen administrativen Aufwand, ohne einen entsprechenden Zugewinn für die Cybersicherheit zu schaffen. Aus Sicht der gewerblichen Wirtschaft sollte daher konsequent der Grundsatz „ein Vorfall, eine Meldung“ gelten. Meldepflichten, Meldeschwellen, Fristen und Datenformate sollten über die verschiedenen Rechtsakte hinweg vollständig harmonisiert werden und über einen einheitlichen Zugangspunkt auf Ebene der Mitgliedstaaten erfolgen. Informationen aus den Meldungen sollten in operativen Nutzen für die Unternehmen umgewandelt werden – etwas durch gezielte Warnhinweise und Handlungsempfehlungen.

- Freiwilligkeit von Zertifizierungen bewahren

Cybersicherheitszertifizierungen können einen wichtigen Beitrag zur Vertrauensbildung und zum Nachweis der Einhaltung regulatorischer Anforderungen leisten. Der Kommissionsvorschlag enthält bereits risikobasierte Ansätze, u. a. eine vereinfachte Selbstbewertung für niedrigere Vertrauensstufen. Die KMU-Tauglichkeit sollte im Gesetzgebungsverfahren weiter abgesichert werden, damit nicht nur größere Unternehmen von der Vermutungswirkung partizipieren.

Die DIHK spricht sich dafür aus, bestehende internationale Standards und Normen als Grundlage heranzuziehen und gleichwertige Zertifizierungen aus vertrauenswürdigen Drittstaaten gegenseitig anzuerkennen. Dadurch können Doppelzertifizierungen vermieden, Kosten reduziert und die internationale Wettbewerbsfähigkeit europäischer Unternehmen gestärkt werden.

Gleichzeitig ist sicherzustellen, dass Zertifizierungssysteme ihren freiwilligen Charakter behalten und nicht faktisch zu einer Voraussetzung für den Marktzugang werden.

- Verhältnismäßigkeit des Hochrisiko-Lieferanten-Regimes

Der vorgeschlagene Rahmen zur Bewertung und gegebenenfalls zum Ausschluss von Hochrisiko-Anbietern greift tief in bestehende Lieferketten ein. Viele Unternehmen sind auf global verzweigte Beschaffungsstrukturen angewiesen. Ein Ausschluss von Anbietern ohne hinreichende und marktfähige Alternativen kann zu erheblichen Mehrkosten, Lieferengpässen und neuen Abhängigkeiten führen. Entsprechende Maßnahmen sollten deshalb ausschließlich auf Grundlage transparenter, objektiver und überprüfbarer Kriterien und belastbarer Folgenabschätzungen getroffen werden.

- Übergangsfristen an Investitionszyklen ausrichten

In zahlreichen Wirtschaftsbereichen sind Investitionen in Infrastruktur, industrielle Anlagen und Produktkomponenten auf langfristige Nutzungs- und Abschreibungszeiträume ausgelegt. Die in Artikel 110 vorgesehene Übergangsfrist von 36 Monaten für den Austausch kritischer Komponenten wird diesen Realitäten vielfach nicht gerecht.

Übergangsfristen sollten stärker an tatsächlichen Investitions- und Nutzungszyklen ausgerichtet werden, um Rechts-, Investitions- und Planungssicherheit für die Unternehmen zu gewährleisten.

- Evaluierung mit Blick auf Praxistauglichkeit und Belastungen

Die Bewertung der Wirksamkeit neuer Regelungen sollte sich nicht ausschließlich am erreichten Sicherheitsniveau orientieren. Ebenso relevant sind ihre praktische Umsetzbarkeit sowie die daraus resultierenden bürokratischen und finanziellen Belastungen für Unternehmen.

Bewertung im Einzelnen

Governance und Rolle der ENISA / Single-Reporting-Struktur

Der CSA 2 soll die Rolle der ENISA deutlich stärken. Konkret ist unter anderem vorgesehen, dass sie stärker operative Aufgaben übernimmt, etwa bei der Koordination auf EU-Ebene, bei der Bereitstellung von Frühwarnungen zu Cyberbedrohungen und bei der Unterstützung im Rahmen von Sicherheitsvorfällen. Dafür sollen auch die Ressourcen der ENISA erhöht werden.

In der Vergangenheit zeigten sich viele Probleme in der Umsetzung des EU-Cybersicherheitsregimes aufgrund unterschiedlicher Interpretationen von Vorgaben und zahlreicher Berichts- und Nachweispflichten. Aus Sicht der gewerblichen Wirtschaft reduzieren einheitliche Auslegungen und Verfahren Rechtsunsicherheiten, senken Compliance-Kosten und erleichtern grenzüberschreitende Geschäftstätigkeit im europäischen Binnenmarkt. Insbesondere für international tätige Unternehmen ist eine harmonisierte Umsetzung von Cybersicherheitsvorgaben ein wichtiger Standort- und Wettbewerbsfaktor. Dafür braucht es Transparenz, Nachvollziehbarkeit und eine enge Orientierung an technischen Standards.

Eine klarere Aufgabenteilung zwischen der ENISA und den nationalen Aufsichtsbehörden und eine stärkere Koordinierungsfunktion der ENISA können dazu beitragen, effizientere Prozesse und mehr Rechtssicherheit zu schaffen. Die Etablierung dieser Prozesse muss im engen Schulterschluss mit den nationalen Cybersicherheitsbehörden erfolgen.

Die ENISA sollte zudem gemeinsam mit den nationalen Sicherheitsbehörden ihre Rolle als Beratungs-, Warn- und Unterstützungsinstanzen für Unternehmen weiter ausbauen. Die Informationsangebote zur Umsetzung des Cyber Resilience Act sind ein guter Ansatz. Die gewerblich Wirtschaft benötigt praxisnahe und rechtssichere Orientierungshilfen. Insbesondere kleine und mittlere Unternehmen sollten dabei durch weitere niedrigschwellige Informations- und Beratungsangebote unterstützt werden.

Die Entwicklung technischer Standards sollte weiterhin im europäischen Normungssystem erfolgen. Die ENISA sollte hierbei beratend und koordinierend tätig sein, jedoch keine

eigenständige normsetzende Funktion übernehmen. Auch hier sollte der Grundsatz der Gewaltenteilung zwischen Normsetzung und Kontrolle der Einhaltung der Normen Anwendung finden.

Eine besonders drängende Neuerung ist die Einrichtung einer einheitlichen Meldestelle für Cybersicherheitsvorfälle. Ziel muss „ein Vorfall, eine Meldung“ sein, denn jede Mehrfachmeldung bindet personelle Ressourcen in Unternehmen, ohne die Cybersicherheit zu erhöhen. Besonders für KMU stellen parallele Meldewege eine erhebliche Belastung dar.

Um dieses Ziel zu erreichen, sollten Meldeschwellen, Fristen, Datenformate und Verfahren über bestehende Rechtsakte hinweg harmonisiert werden, insbesondere zwischen NIS-2, CER-Richtlinie, Datenschutzrecht, Cyber Resilience Act und weiteren sektorspezifischen Cybersicherheitsvorgaben wie Vigilanzmeldungen nach MDR/IVDR über EUDAMED.

Unternehmen sollten sicherheitsrelevante Vorfälle grundsätzlich nur einmal gegenüber ihrer zuständigen nationalen Behörde melden müssen. Die Einführung eines zentralen Meldeportals darf nicht zu zusätzlichen Berichtspflichten auf europäischer Ebene führen. Ein solcher Single Entry Point sollte daher vorrangig national verankert werden. Nationale Behörden bzw. nationale Meldestellen müssen zentrale Ansprechpartner für Unternehmen bleiben. Eine unmittelbare Zentralisierung sensibler Sicherheits- und Vorfalldaten auf EU-Ebene sollte vermieden werden, um keinen zusätzlichen europäischen Single Point of Failure zu schaffen.

Die Weiterleitung an alle weiteren zuständigen Stellen – einschließlich Datenschutzaufsichtsbehörden, Marktüberwachungsstellen sowie der CRA-Meldeplattform – muss behördenseitig über die Single-Reporting-Struktur erfolgen (Once-Only-Prinzip). Meldeformate sollten so gestaltet sein, dass eine Meldung die Pflichtinhalte aller einschlägigen Rechtsakte abdecken kann.

Zugleich sind höchste Anforderungen an Datensicherheit, Zugriffsschutz und Zweckbindung zu stellen. Es muss klar geregelt werden, wie Geschäftsgeheimnisse, Informationen zu laufenden Angriffen, Schwachstelleninformationen und sonstige sensible Unternehmensdaten geschützt werden, welche Stellen auf welche Daten zugreifen dürfen und welche Informationen anonymisiert oder weitergegeben werden dürfen.

Zudem ist ein wesentlicher Faktor für die Akzeptanz der Meldepflichten, dass diese in klaren operativen Nutzen für die Unternehmen umgewandelt werden. Dazu gehören aktuelle Lagebilder, technische Warnungen und Handlungsempfehlungen sowie der Zugang zu behördlicher oder staatlich koordinierter Unterstützung bei der Analyse und Bewältigung schwerwiegender Cybervorfälle. ENISA-Leistungen wie Frühwarnungen, Schwachstellendatenbank und Ransomware-Unterstützung müssen so aufbereitet werden, dass auch Unternehmen ohne eigenes Security Operations Center sie unmittelbar nutzen können: maschinenlesbar über standardisierte Schnittstellen, mehrsprachig und mit priorisierten Handlungsempfehlungen. Der

geplante Ransomware-Helpdesk und die Unterstützung bei der Vorfallsbewältigung sollten KMU ausdrücklich offenstehen.

Reform des Europäischen Rahmens für Cybersicherheitszertifizierungen (ECCF)

Die Reform des Europäischen Rahmens für Cybersicherheitszertifizierungen (ECCF) soll vor allem beschleunigte Verfahren und mehr Harmonisierung bringen. Zertifizierungsverfahren sollen künftig vereinfacht und stärker zentral koordiniert werden, sodass Produkte und Dienste "secure-by-design" in den Markt gelangen und Zertifizierung verstärkt als Nachweisinstrument für die Einhaltung regulatorischer Vorgaben dienen kann.

Nach Ansicht der DIHK kann ein einheitlicher europäischer Zertifizierungsrahmen bei richtiger Ausgestaltung zu einem wichtigen Wettbewerbsfaktor für den digitalen Binnenmarkt werden. Unternehmen profitieren von geringeren Transaktionskosten, mehr Rechtssicherheit und einer besseren Skalierbarkeit digitaler Produkte und Dienstleistungen innerhalb der EU. Der CSA 2 darf dabei jedoch keine neuen Anforderungen an Produkte mit eigenem Konformitätsregime öffnen, beispielsweise für digitale Medizinprodukte, für die die Medical Device Regulation (MDR) das maßgebliche Produktsicherheitsregime bleibt.

Europäische Cybersicherheitszertifikate sollten als Nachweis zur Einhaltung von Sicherheitsanforderungen anerkannt werden, um Doppelprüfungen zu vermeiden. Dies ist insbesondere hinsichtlich der Organisations-Nachweise für NIS-2 und der Nachweise technischer Sicherheitsanforderungen für den Cyber Resilience Act sinnvoll, sollte aber ausdrücklich auch sektorale Regime einschließen (etwa die Cybersicherheitsanforderungen der MDR), des Datenschutzrechts und des AI Acts für Hochrisiko-KI-Systeme. Ein europäisches Cybersicherheitszertifikat sollte von Benannten Stellen, Aufsichtsbehörden und Auftraggebern als Nachweis der abgedeckten Anforderungen anerkannt werden müssen. Nur so entsteht die angestrebte ‚gemeinsame Sprache‘ zwischen den Rechtsakten, und nur so amortisieren sich Zertifizierungskosten auch für kleinere Hersteller über mehrere Nachweispflichten hinweg.

Bereits bestehende sektorale Zertifizierungen, Audits und Konformitätsbewertungen sollten als Nachweiselemente in europäischen Zertifizierungsschemata systematisch wiederverwendet werden („one audit, multiple use“). Zusätzliche Prüfungen sollten sich nur auf bislang nicht abgedeckte Anforderungen beschränken.

Dabei sollten europäische Zertifizierungen konsequent auf bestehenden internationalen Normen aufbauen. Der europäische Zertifizierungsrahmen sollte zudem Mechanismen zur Anerkennung gleichwertiger Zertifizierungen aus vertrauenswürdigen Drittstaaten vorsehen. Ebenso wichtig ist die Anerkennung europäischer Zertifikate in Drittmärkten. Die Kommission sollte gegenseitige Anerkennungsabkommen (u. a. mit den USA, dem Vereinigten Königreich und Japan) aktiv verfolgen, damit exportorientierte europäische Hersteller – auch KMU mit weltweitem Vertrieb – ihre EU-Zertifikate international verwerten können und nicht je

Zielmarkt erneut prüfen lassen müssen. Dadurch lassen sich Doppelaufwände für Unternehmen vermeiden und die internationale Wettbewerbsfähigkeit europäischer Unternehmen stärken.

Zertifizierungssysteme sollten dabei nach Ansicht der Unternehmen ihren freiwilligen Charakter behalten und nicht faktisch zu einer Voraussetzung für den Marktzugang werden. Verpflichtende Zertifizierungen können dazu führen, dass Ressourcen von echtem Risikomanagement zu formaler Compliance verlagert werden – bei einem Instrument, dessen Wirksamkeit noch nicht erprobt ist. Neue Pflichtzertifizierungen sollten nur eingeführt werden, wenn ihre Wirksamkeit belegt, ihr Verhältnis zu bestehenden Nachweisen geklärt und der zusätzliche Ressourcenaufwand verhältnismäßig ist.

Eine faktische Pflicht kann insbesondere über die Beschaffungspraxis drohen. Öffentliche und private Auftraggeber – etwa NIS-2-Einrichtungen – dürfen nicht durch unklare Lieferkettenpflichten dazu gedrängt werden, pauschal Zertifikate der höchsten Vertrauensstufe von sämtlichen Zulieferern zu verlangen. Vorgaben an Betreiber müssen so gefasst sein, dass risikoadäquate, abgestufte Nachweise (einschließlich Selbsterklärungen und Herstellererklärungen für niedrige Risikoklassen) ausreichen. Umgekehrt gilt: Wo ein Zertifikat vorliegt, muss es individuelle Sicherheitsfragebögen und Einzelaudits der Auftraggeber ersetzen können.

In regulierten Sektoren mit eigenständigen Konformitätsregimen sollte die bestehende regulatorische Konformität grundsätzlich als wesentlicher Sicherheitsnachweis anerkannt werden.

Um die Fragmentierung des Binnenmarktes zu verhindern, sollte von nationalen Zertifizierungspflichten abgesehen werden. Abweichungen vom Grundsatz freiwilliger Zertifizierungen sollten ausschließlich auf Unionsebene festgelegt werden können.

Einzelne Unternehmen weisen darauf hin, dass das europäische Cloud-Zertifizierungsschema (EUCS) unter dem neuen Rahmen prioritär und auf Basis internationaler Normen (ISO/IEC 27001/27017, C5) abgeschlossen werden sollte. Ihrer Ansicht nach sollten Souveränitätsanforderungen und Datenlokalisierungsauflagen, soweit politisch gewollt, als transparente, optionale Zusatzstufe ausgestaltet werden und nicht als Eintrittshürde für alle Vertrauensstufen. Gerade europäische Cloud-KMU benötigen Rechtssicherheit, welche Anforderungen für welche Stufe gelten, und ein Schema, dessen Auditkosten für kleine Anbieter tragbar sind.

Neue Regeln zum Schutz der Lieferketten

Das politisch am stärksten diskutierte Element des neuen CSA 2-Vorschlags ist der vorgeschlagene Rahmen für sichere IKT-Lieferketten in bestimmten Sektoren, die im Wesentlichen bereits NIS2-reguliert sind. Als Grundlage dienen Risikobewertungen und die Benennung von Hochrisiko-Drittländern/-anbietern durch die EU-Kommission. Für Zulieferer aus entsprechend eingestuften Ländern kann dann beispielsweise der Ausschluss von Vergabeverfahren der

öffentlichen Hand oder gar von privaten Unternehmen drohen. Zudem ist in bestimmten Fällen (5G-, Fest- und Satellitennetze) ein verpflichtender Ausstieg aus Hochrisiko-Komponenten für europäische Unternehmen vorgesehen. Der Vorschlag schafft damit erstmals einen horizontalen EU-weiten Rahmen zur Bewertung strategischer und nicht-technischer Risiken in IKT-Lieferketten.

Der vorgeschlagene High-Risk-Supplier-Ansatz als Regelinstrument der europäischen Cybersicherheitspolitik stellt aus Sicht der gewerblichen Wirtschaft einen erheblichen Eingriff in den Markt dar. Eingriffe in bestehende Lieferketten haben unmittelbare Auswirkungen auf Investitionsentscheidungen, Innovationszyklen und die Versorgungssicherheit kritischer Infrastrukturen. Werden Anbieter ausgeschlossen, ohne dass ausreichend marktfähige Alternativen verfügbar sind, können zusätzliche Kosten, Verzögerungen sowie neue Konzentrations- und Abhängigkeitsrisiken entstehen.

Sektorspezifische Sonderregelungen etwa für die Telekommunikationsbranche sowie pauschale „Rip-and-Replace“-Verpflichtungen sollten vermieden werden. Eine gegenüber anderen kritischen Sektoren abweichende Behandlung einzelner Sektoren bedarf einer besonderen sachlichen Rechtfertigung und einer belastbaren, sektorspezifischen Folgenabschätzung.

Ziel europäischer Cybersicherheitspolitik sollte daher nicht nur die Risikoreduzierung sein, sondern zugleich die Stärkung technologischer Resilienz und Wettbewerbsfähigkeit Europas.

Voraussetzung für einen verhältnismäßigen Einsatz sind:

1. transparente Kriterien für die Einstufung von Hochrisikostaat und Unternehmen

Die Einstufung von Hochrisiko-Anbietern sollte auf objektiven, transparenten und überprüfbaren Kriterien beruhen. Dafür bedarf es eines verbindlichen, EU-weit einheitlichen Bewertungsverfahrens. Einheitliche Standards, Methoden und Fristen sollten sicherstellen, dass alle Mitgliedstaaten Risiken gleich bewerten und Maßnahmen koordiniert umsetzen und so die Fragmentierung des Binnenmarkts weiter reduziert wird.

Für Produkte, die bereits einem sektorspezifischen europäischen Konformitätsbewertungsregime unterliegen, insbesondere nach MDR und In-vitro Diagnostic Medical Devices Regulation (IVDR), sollte der CSA 2 ausdrücklich klarstellen, dass keine zusätzlichen produktbezogenen Anforderungen oder Nachweispflichten begründet werden. Zudem sollte das Verhältnis zwischen Maßnahmen gegenüber Hochrisiko-Anbietern und bereits erfolgten Konformitätsbewertungen durch Benannte Stellen widerspruchsfrei geregelt werden.

2. differenzierte Risikoanalysen und Folgenabschätzung

Maßnahmen wie Beschränkungen oder Austauschpflichten sollten nur dort zur Anwendung kommen, wo konkrete Risiken nachvollziehbar belegt sind und verhältnismäßig adressiert

werden können. Eine pauschale oder politisch motivierte Anwendung solcher Instrumente würde die Planungs- und Investitionssicherheit der Unternehmen beeinträchtigen.

Der Anwendungsbereich verpflichtender Maßnahmen im Rahmen sicherer IKT-Lieferketten sollte grundsätzlich auf besonders kritische Sektoren beschränkt werden, in denen Cybervorfälle erhebliche gesellschaftliche oder wirtschaftliche Auswirkungen entfalten können.

Der sachliche Anwendungsbereich sollte sich an den Ergebnissen koordinierter Risikobewertungen orientieren. Für den Telekommunikationsbereich beispielsweise bedeutet dies, dass verpflichtende Maßnahmen auf nachweislich kritische Funktionen wie Kernnetzsysteme begrenzt bleiben. Eine undifferenzierte Einbeziehung des gesamten Radio Access Network sowie von Fest- und Satellitennetzen ist ohne eine vergleichbare Risikobewertung nicht sachgerecht.

Beschränkungen, Nutzungsverbote oder Austauschverpflichtungen sollten ausdrücklich nur als ultima ratio vorgesehen werden und erst greifen, wenn konkrete Risiken nachgewiesen sind und keine gleich wirksamen risikomindernden Maßnahmen zur Verfügung stehen. Vorrangig sind mildere Risikominderungsmaßnahmen zu prüfen und zu berücksichtigen.

Bei der Bewertung von Lieferkettenrisiken sollten bestehende Risikominderungsmaßnahmen der Unternehmen ausdrücklich berücksichtigt werden. Hierzu zählen insbesondere Diversifizierungsstrategien, Multi-Vendor-Ansätze, Segmentierung kritischer Systeme sowie organisatorische und technische Sicherheitsmaßnahmen. Regulatorische Eingriffe sollten diese Instrumente nicht verdrängen, sondern vorrangig auf ihnen aufbauen. Regulatorik sollte innovationsbasierte Sicherheitsansätze unterstützen wie die Entwicklung offener Netzarchitekturen, statt auf ein rein hardwarebezogenes „Rip & Replace“.

Sollten Hochrisiko-Anbieter benannt und Abhilfemaßnahmen getroffen werden, sollten vorher unionsweit nachvollziehbare Risiko-, Kosten- und Folgenabschätzungen durchgeführt werden. Dabei sollten die betroffenen Sektoren verbindlich angehört und insbesondere die Auswirkungen auf Versorgungssicherheit, Wettbewerb, Innovationsfähigkeit und Investitionsplanung berücksichtigt werden. Insbesondere in stark regulierten Sektoren wie dem Gesundheitswesen kann der Austausch einzelner Komponenten umfangreiche Re-Zertifizierungs- oder Änderungsverfahren auslösen. Folgenabschätzungen sollten deshalb ausdrücklich die Auswirkungen auf Versorgungssicherheit, (Patienten-)Sicherheit sowie bestehende regulatorische Zulassungs- und Zertifizierungsverfahren berücksichtigen. Eine Verfügbarkeitsprüfung von Alternativen könnte als Voraussetzung vor den Ausschluss von Anbietern gestellt werden.

Die Folgenabschätzung sollte zusätzlich belastbare Zeit- und Umsetzungsschätzungen umfassen, darunter Genehmigungs-, Beschaffungs-, Integrations-, Zertifizierungs- und Migrationszeiten. Bereits vereinbarte nationale Migrationspfade und nachweisbare Investitionen der Betreiber sind dabei ausdrücklich zu berücksichtigen.

3. Vermeidung von Marktverwerfungen und Unterstützung europäischer Alternativen

Sofern die Europäische Union bestimmte Anbieter aus Sicherheitsgründen beschränken möchte, muss dies aktiv flankiert werden. Sicherheitsziele und wirtschaftliche Handlungsfähigkeit sollten miteinander in Einklang stehen. Versorgungssicherheit sollte jederzeit gewährleistet sein. Verbote oder Beschränkungen sollten nur dann verhältnismäßig sein, wenn ausreichend verfügbare, sichere, leistungsfähige und wirtschaftlich tragfähige Alternativen bestehen. Andernfalls drohen Preissteigerungen, Lieferengpässe, Marktkonzentrationen und neue Abhängigkeiten, die ihrerseits die Resilienz schwächen können.

Bei den flankierenden Maßnahmen sollte daher insbesondere darauf geachtet werden, europäische Alternativen aufzubauen und europäische Kapazitäten langfristig zu stärken. Der Vorschlag sollte mit Programmen ergänzt werden, die Forschung und Entwicklung europäischer Hersteller fördern, Diversifizierung unterstützen und Unternehmen beim Übergang zu alternativen Anbietern helfen. Damit europäische Alternativen schneller auf den Markt kommen können, sind unbürokratische Maßnahmen notwendig. Dazu zählen vor allem verschlankte und beschleunigte Begutachtungs- und Bewilligungsverfahren, die den Aufwand für innovative KMU und Start-ups verringern und bürokratische Hürden abbauen. Einige Unternehmen sprechen sich außerdem dafür aus, den Aufbau eigener technologischer Fähigkeiten stärker zu unterstützen.

4. ausreichende Übergangsfristen

Der CSA 2 (Artikel 110) sieht Übergangsfristen (36 Monate) für den Austausch kritischer Komponenten vor. Unternehmen treffen Investitionsentscheidungen in kritischen Infrastrukturen häufig auf Grundlage mehrjähriger bis mehr als zehnjähriger Planungs- und Nutzungszyklen. Neue regulatorische Anforderungen sollten daher Übergangszeiten, bestehende Investitionen und bereits laufende Umsetzungsmaßnahmen angemessen berücksichtigen, um Rechts- und Planungssicherheit zu gewährleisten. In langzyklischen OT- und KRITIS-Infrastrukturen sollten Austauschpflichten möglichst mit ohnehin anstehenden Erneuerungs-, Modernisierungs- oder Rezertifizierungszyklen synchronisiert werden. Insgesamt ist entscheidend, dass Maßnahmen operativ umsetzbar bleiben und die Realität globaler Wertschöpfungsketten berücksichtigt wird. Übergangsfristen dürfen daher nicht schematisch festgelegt werden, sondern müssen sich an den realen technischen und wirtschaftlichen Lebenszyklen der betroffenen Komponenten orientieren.

Eine weitere Verkürzung der Frist, insbesondere auf 24 Monate wie vom ITRE-Ausschuss gefordert, wäre nicht operativ umsetzbar. Für komplexe Telekommunikationsnetze beispielsweise würde ein vollständiger Austausch 7 bis 10 Jahre dauern. Allein behördliche Genehmigungen erfordern 6 bis 12 Monate, die Auswahl geeigneter Hersteller 1 bis 2 Jahre, die Zertifizierung von Komponenten bis zu einem Jahr. Fristen sollten anhand technischer Migrationspläne, verfügbarer Alternativen und regulärer Modernisierungszyklen festgelegt werden. Soweit ein vollständiger Austausch erforderlich ist, sollte eine deutlich längere,

einzelfallbezogene Übergangsfrist vorgesehen werden. Nationale Migrationspfade und bereits getätigte Investitionen der betroffenen Unternehmen sollten berücksichtigt werden.

5. Schutz von KMU-Zulieferern vor ungefilterter Pflichten-Kaskadierung

Die im Zusammenhang mit den Lieferketten vorgesehenen Pflichten richten sich zwar formal an Betreiber kritischer Infrastrukturen, entfalten jedoch faktisch Auswirkungen entlang der gesamten Zulieferkette. In der Praxis ist zu beobachten, dass regulatorische Anforderungen häufig unverändert und über die eigentlichen Vorgaben hinausgehend an Zulieferer weitergegeben werden. Der CSA sollte daher klarstellen, dass

- Transparenz- und Nachweispflichten von Zulieferern auf den jeweiligen Liefergegenstand sowie dessen tatsächlichen Beitrag zum Risikoprofil begrenzt bleiben müssen,
- standardisierte und EU-weit einheitliche Nachweisformate (z. B. Herstellererklärungen, Software Bill of Materials (SBOM) oder gegebenenfalls Zertifikate) individuelle Auditrechte und umfangreiche Fragebögen grundsätzlich ersetzen sollten, um unnötigen bürokratischen Aufwand zu vermeiden,
- KMU-Zulieferer, die selbst nicht als Hochrisiko-Anbieter eingestuft sind, nicht allein aufgrund von Unterlieferantenbeziehungen pauschal ausgeschlossen werden dürfen, sofern sie angemessene Prüf-, Risiko- und Diversifizierungsmaßnahmen nachweisen können.

Sanktionsrahmen

Der vorgesehene umsatzbezogene Sanktionsrahmen (bis zu 1 % des weltweiten Jahresumsatzes bei Transparenzverstößen, bis zu 7 % bei Verstößen gegen Nutzungsverbote) muss verhältnismäßig ausgestaltet werden.

Erforderlich sind eine klare Abstufung nach Schwere, Verschulden und Unternehmensgröße, ein Vorrang von Anordnung und Nachbesserung vor Bußgeld („Beraten vor Strafen“, insbesondere bei Erstverstößen von KMU) sowie Rechtssicherheit darüber, welche Prüf- und Dokumentationstiefe von Unternehmen welcher Größe erwartet wird.

Evaluierung

Die Wirksamkeit der Regelungen sollte regelmäßig – erstmals drei Jahre nach Geltungsbeginn – evaluiert werden, insbesondere im Hinblick auf ihre Praxistauglichkeit, ihre Auswirkungen auf die Wettbewerbsfähigkeit der Unternehmen und die mit ihrer Umsetzung verbundenen bürokratischen und finanziellen Belastungen.

Dabei sollten die Compliance-Kosten für KMU gesondert erhoben (KMU-Test) und stark regulierte Sektoren, in denen mehrere Cybersicherheits- und Produktsicherheitsregime kumulieren, gesondert betrachtet werden. Zeigt sich, dass Zertifizierungen faktisch zur

Marktzugangsvoraussetzung geworden sind oder KMU systematisch aus Lieferketten gedrängt werden, sind Gegenmaßnahmen zu ergreifen.

Ansprechpartner

Dr. Katrin Sobania

Leiterin des Referats Informations- und Kommunikationstechnologie, E-Government, Postdienste, Daten- und Informationssicherheit

Tel +49 30 20308-2109, sobania.katrin@dihk.de

Jonas Wöll

Referatsleiter Digitaler Binnenmarkt, EU-Verkehrspolitik, Regionale Wirtschaftspolitik

Tel: +49 151 1131483, woell.jonas@dihk.de

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein. Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zum Gesamtinteresse der gewerblichen Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage unserer Stellungnahmen sind die wirtschaftspolitischen Positionen und beschlossenen Positionspapiere der DIHK unter Berücksichtigung der der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs und ihrer Mitgliedsunternehmen.

Darüber hinaus koordiniert die DIHK das Netzwerk der 150 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 93 Ländern.

Die DIHK ist im Transparenzregister der Europäischen Union unter der Nummer 22400601191-42 registriert.