

Positionspapier der ISPA

zum Vorschlag der Europäischen Kommission für einen EU Cybersecurity Act (CSA 2)

13. April 2026

Der von der Europäischen Kommission vorgelegte Entwurf zur Überarbeitung des EU Cybersecurity Act (CSA2) verfolgt das wichtige Ziel, ein unionsweit hohes Cybersicherheitsniveau sicherzustellen und die Resilienz kritischer digitaler Infrastrukturen zu stärken. In seiner derzeitigen Ausgestaltung wirft der Vorschlag jedoch erhebliche rechtliche, technische und wirtschaftliche Bedenken auf. Insbesondere im Bereich der Lieferkettensicherheit sowie im Hinblick auf die vorgesehenen Zertifizierungsmechanismen besteht grundlegender Überarbeitungsbedarf.

1. Sicherheit in IKT-Lieferketten und Einstufung als Hochrisikolieferanten

Der CSA 2 sieht vor, Lieferanten anhand pauschaler Kriterien als „Hochrisiko“ einzustufen – unter anderem aufgrund ihres Sitzstaates oder anderer nichttechnischer Merkmale. Eine solche Klassifizierung hätte weitreichende Folgen: verpflichtende Ausschlüsse aus Lieferketten, der Verlust von Zertifizierungsmöglichkeiten, Beschaffungsverbote für NIS2-regulierte Unternehmen sowie umfangreiche Austauschpflichten in bestehenden Netzen. Diese Eingriffe bergen erhebliche wirtschaftliche und sogar technische Risiken, insbesondere für Betreiber kritischer digitaler Infrastrukturen. Eine überhastete oder einseitige EU-Regulierung birgt zudem das Risiko, nationale Entscheidungssouveränität und strategische Handlungsspielräume zu beschneiden und damit Österreichs Fähigkeit zu schwächen, eigene netzpolitische, wirtschaftliche und sicherheitsrelevante Interessen sowie seine langfristige Innovations- und Standortattraktivität selbstbestimmt zu gestalten.

a) Problemendarstellung

Für eine sachgerechte Bewertung von Risiken in der IKT-Lieferkette ist es unerlässlich, dass Entscheidungen ausschließlich auf technisch überprüfbaren, nachvollziehbaren und verhältnismäßigen Kriterien beruhen. Eine Hochrisikoeinstufung von Lieferanten kann bei betroffenen Betreibern erhebliche Mehrkosten verursachen – etwa durch notwendige Anpassungen oder den Austausch von Komponenten. Solche Austauschprozesse sind im TK-Bereich oft technisch komplex, betreffen mehrere abhängige Systeme gleichzeitig und führen damit zu erheblich höheren Gesamtkosten als von der Kommission bislang angenommen. Zusätzlich sind Lieferengpässe wahrscheinlich, da für zentrale Netzkomponenten begrenzte Produktionskapazitäten verfügbar und lange Vorlaufzeiten zu befürchten sind. Diese Faktoren erhöhen das Risiko, dass die tatsächlichen Kosten ein Vielfaches der bisherigen Schätzungen erreichen, was in der Praxis entweder zu höheren Belastungen für Endnutzerinnen und Endnutzer führt oder dazu, dass notwendige Investitionen zurückgestellt werden – mit entsprechenden negativen Folgen für Innovation

und Ausbau. Gleichzeitig führt eine Verengung des Lieferantenfeldes zwangsläufig zu weniger Wettbewerb, was höhere Beschaffungspreise und langsamere technologische Entwicklungen begünstigt und die Verhandlungsposition europäischer Betreiber zusätzlich schwächt. Zudem ist zu berücksichtigen, dass neue Abhängigkeiten von einzelnen Anbietern sowie die Entstehung von Monopolstellungen vermieden werden sollten, um einen fairen Wettbewerb und eine resiliente Marktstruktur langfristig zu sichern. Maßnahmen müssen daher sorgfältig abgewogen werden, um wirtschaftliche Belastungen ebenso zu berücksichtigen wie mögliche Auswirkungen auf die Versorgungssicherheit. Ein Ansatz, der geopolitische oder andere nicht technische Erwägungen in den Vordergrund stellt, ist aus Sicht der ISPA nicht geeignet. Denn dies steht im Widerspruch zum risikobasierten Grundprinzip der europäischen Cybersicherheitsregulierung und birgt die Gefahr sachfremder Entscheidungen, die keinen Bezug zur tatsächlichen Sicherheit aufweisen.

b) Lösung: Technischer Fokus und bewährte nationale Mechanismen

Die österreichische und europäische Regulierungspraxis zeigt, dass bereits funktionierende, technisch fundierte Mechanismen bestehen. Mit Inkrafttreten des NISG 2026 werden Sicherheitsanforderungen entlang der gesamten Lieferkette nochmals verschärft und gewährleisten bereits ein hohes Schutzniveau. Der Netzsicherheitsbeirat, eingerichtet durch das TKG 2021, überwacht kontinuierlich die Sicherheit von Netzkomponenten und Herstellern. Die bisherigen Evaluierungen haben wiederholt gezeigt, dass kein zusätzlicher regulatorischer Eingriff erforderlich war.

Cybersecurity ist das Produkt von konsequenten technischen und organisatorischen Sicherheitsmaßnahmen. Nicht-technische Risiken – etwa potenzielle staatliche Einflussnahmen, Sabotage oder Datenabflüsse – können effektiv nur durch robuste technische Vorkehrungen adressiert werden. Hierzu zählen insbesondere:

- Zero-Trust-Architekturen
- Strikte Zugriffskontrollen
- Kontinuierliches Monitoring und unabhängige Sicherheitsprüfungen

Besonders im Hinblick auf sogenannte „Kill-Switch“-Szenarien oder Spionageaktivitäten ist entscheidend, dass nicht die Herkunft eines Herstellers, sondern nur die grundsätzliche technische Gestaltung der Netzarchitektur die Resilienz sicherstellen können. Durch geeignete Systemdesigns muss gewährleistet sein, dass einzelne Komponenten keine systemkritischen Ausfallwirkungen entfalten können. Eine diversifizierte und resilient gestaltete Infrastruktur ist der zentrale Ansatz - nicht der pauschale Ausschluss einzelner Anbieter.

Ein weiteres wesentliches Sicherheitsziel ist die Dienstkontinuität. Umfangreiche oder zeitkritische Austauschmaßnahmen erhöhen den Betriebsaufwand und können

Unterbrechungen oder Qualitätsverluste verursachen. Diese Migrationsrisiken müssen daher integraler Bestandteil der Risikobewertung sein, insbesondere bei kritischen Netzinfrastrukturen. Diese Faktoren würden Ausbauziele massiv verzögern und die Netzstabilität im Übergang negativ beeinflussen.

Im Vordergrund sollten weiterhin technische Maßnahmen stehen, die unabhängig von einzelnen Herstellern und derer geographischer Herkunft wirksam sind. Dazu gehören segmentierte Netzarchitekturen, beschränkte Kommunikationspfade, gesicherte administrative Zugänge sowie unabhängige Prüf- und Überwachungsmechanismen. Ergänzend sollte ein risikobasiertes Integrationsmodell verfolgt werden, das definiert, unter welchen technischen und organisatorischen Bedingungen Komponenten sicher eingebunden werden können.

Die ISPA fordert daher:

- Ein **objektives, ausschließlich technisch begründetes Verfahren** zur Einstufung von Lieferanten und **keine politisch motivierte Benachteiligung einzelner Hersteller**.
- Einheitliche, EU-weit abgestimmte Kriterien und Prozesse, um widersprüchliche Vorgaben zu vermeiden und **keine zusätzlichen Aufsichtsstrukturen** zu schaffen.
- Den Verzicht auf pauschale Austauschpflichten, da diese nicht nur potenziell Netzunterbrechungen verursachen, sondern auch deutlich höhere Kosten als bislang angenommen nach sich ziehen, den Wettbewerb verzerren und die Innovationskraft erheblich einschränken.
- Ein risikobasiertes Integrationsmodell, das klare technische Voraussetzungen für den sicheren Einsatz von Komponenten definiert.

2. Zertifizierungsframework (ECCF)

a) Problemdarstellung

Unternehmen, die als wesentliche oder wichtige Einrichtungen nach der NIS-2-Richtlinie reguliert sind, erfüllen bereits umfassende Vorgaben zu Cybersicherheit, Risiko und Schwachstellenmanagement, Audits, Dokumentation und Kontrolle. Dies betrifft insbesondere Telekommunikationsunternehmen, deren Kommunikationsnetze als kritische Infrastrukturen besonders strengen Anforderungen unterliegen.

Im Zuge der zunehmenden Komplexität moderner Netze entwickeln Betreiber seit Jahren eigene Software ausschließlich für den internen Einsatz oder den Einsatz in der Unternehmensgruppe, etwa für Monitoring, Management oder Orchestrierung in Zugangs- und Kernnetzen. Diese Anwendungen entstehen in streng gesicherten und regelmäßig geprüften Umgebungen – insbesondere im Rahmen der NIS2-Aufsicht sowie häufig auf Basis von ISO 27001. Eine zusätzliche Zertifizierungspflicht nach dem ECCF für solche eigenentwickelten, nicht am Markt bereitgestellten Produkte und Prozesse

würde keinen zusätzlichen Sicherheitsgewinn erzeugen, sondern bestehende Pflichten lediglich duplizieren. Hinzu kommt, dass der CSA 2 mit der „CyberPosture“-Zertifizierung bereits eine umfassende externe Bewertung der gesamten Einrichtung vorsieht. Entwicklung und Betrieb eigener Software erfolgen damit ohnehin innerhalb von Organisationen, die selbst nach einem extern geprüften Schema zertifiziert werden müssen. Eine zusätzliche Produktzertifizierung würde dieser Systematik widersprechen und die geforderte strukturelle Unabhängigkeit der Prüfstellen unterlaufen, weil Betreiber ihre eigenen Produkte nicht gleichzeitig selbst zertifizieren können. Vor diesem Hintergrund erscheint eine weitere Zertifizierung von Eigenentwicklungen weder zweckmäßig noch verhältnismäßig.

b) Lösungsvorschlag:

Damit Zertifizierungen in der Praxis tatsächlich zur Sicherheit beitragen und nicht zu unnötigen Belastungen führen, müssen sie klar auf ihren Zweck ausgerichtet bleiben. Wichtig ist, dass keine faktischen Pflichtzertifizierungen entstehen, etwa durch Markt- oder Zulassungsvoraussetzungen, die über den eigentlichen Regelungszweck hinausgehen. Ebenso wesentlich ist eine enge Abstimmung mit bestehenden Sicherheitsstandards und Prüfmechanismen, damit keine parallelen oder widersprüchlichen Anforderungen entstehen. Dazu zählen insbesondere etablierte Normen wie ISO 27001 sowie bereits bestehende Prüfprozesse im Rahmen der NIS-2-Aufsicht.

Für Betreiber digitaler Infrastrukturen ist zudem entscheidend, dass Zertifizierungs-, Melde- und Aufsichtsverfahren systematisch aufeinander abgestimmt sind. Vorgaben aus CSA, DNA, NIS2, RKEG, dem CRA, oder dem Datenschutzrecht sollen nicht voneinander abweichen oder zu kumulativen Berichts- und Zertifizierungspflichten führen. Meldeschwellen und Kriterien sollten daher so weit wie möglich harmonisiert werden, und pro Mitgliedstaat sollte ein einheitliches Meldesystem vorgesehen werden. Europäische Vereinheitlichungen wie zentrale Meldestellen und kohärente Aufsichtsstrukturen sind grundsätzlich zu begrüßen, müssen aber bestehende Prozesse konsistent ergänzen und dürfen keine zusätzlichen administrativen Belastungen erzeugen.

Die ISPA fordert daher:

- Eine gesetzliche Ausnahme für ICT-Produkte, Dienste und Prozesse, die von NIS2 regulierten Unternehmen ausschließlich für den Eigenbetrieb oder den Betrieb in der Unternehmensgruppe entwickelt und eingesetzt werden.
- Die Anerkennung bestehender Zertifizierungen auf EU-Ebene, sofern sie ein gleichwertiges Schutzniveau gewährleisten.
- Eine enge Abstimmung von Zertifizierungsanforderungen mit bereits bestehenden Cybersecurity Melde- und Aufsichtsprozessen, damit keine redundanten Prüfungen oder zusätzlichen Nachweispflichten entstehen.

3. Schlussfolgerung

Der CSA2 bedarf einer grundlegenden Überarbeitung. Notwendig ist eine klare Fokussierung auf **technische, risikobasierte Sicherheitskriterien**, die Vermeidung politisch motivierter Markteingriffe und die konsequente Anerkennung bestehender Zertifizierungen. Nur so kann ein hohes Cybersicherheitsniveau erreicht werden, ohne gleichzeitig die Wettbewerbsfähigkeit des europäischen IKT-Sektors zu gefährden. Die ISPA unterstützt einen ganzheitlichen, evidenzbasierten Ansatz, der technische Resilienz, Diversifizierung und regulatorische Effizienz vereint.

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 220 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.