Cyber Security Act II

Telekommunikationsinfrastruktur und Sicherheit in der Lieferkette

Der Verband Alternativer Telekom-Netzbetreiber (VAT) begrüßt die Zielsetzung des vorgeschlagenen Cyber Security Act 2, das Cybersicherheitsniveau in der Europäischen Union weiter zu erhöhen und die Resilienz digitaler Lieferketten zu stärken. Eine leistungsfähige, sichere und verlässliche digitale Infrastruktur bildet die Grundlage für wirtschaftliche Entwicklung, gesellschaftliche Stabilität sowie die digitale Souveränität Europas.

Aus Sicht des VAT ist jedoch entscheidend, dass neue regulatorische Vorgaben praxisnah, verhältnismäßig und technologieneutral ausgestaltet werden. Sicherheitsanforderungen müssen sich an objektiven, technisch nachvollziehbaren Kriterien orientieren und dürfen bestehende, bewährte Infrastrukturen nicht unverhältnismäßig beeinträchtigen.

Globale Lieferketten im Telekommunikationssektor

Gerade im Bereich der Telekommunikationsinfrastruktur ist Europa in hohem Maße in globale Lieferketten eingebunden. Die bestehenden Netze sind über Jahrzehnte gewachsen, technisch hochkomplex und beruhen auf einer Vielzahl spezialisierter Komponenten. In zentralen Netzbereichen, insbesondere bei Core-Netz-Komponenten, kommt einzelnen Anbietern aufgrund ihrer technologischen Leistungsfähigkeit, Innovationskraft, Skalierbarkeit und Marktverfügbarkeit erhebliche Bedeutung zu. Für zahlreiche Mitgliedsunternehmen des VAT stellen Produkte dieser Anbieter einen integralen Bestandteil der bestehenden Netzinfrastruktur dar. Ein kurzfristiger Austausch ist faktisch nicht möglich bzw. nur unter erheblichen technischen, wirtschaftlichen und operativen Auswirkungen realisierbar.

Vor diesem Hintergrund sieht der VAT pauschale oder faktisch erzwungene Ausschlüsse einzelner Lieferanten, etwa durch eine Einstufung als „Hochrisikoanbieter“, kritisch. Ein regulatorisch veranlasster Lieferantenwechsel würde erhebliche wirtschaftliche Belastungen verursachen, laufende Ausbauprojekte verzögern und bestehende Investitionsplanungen untergraben. Angesichts der begrenzten Zahl technologisch gleichwertiger Anbieter hätte der Ausschluss eines Unternehmens zudem spürbare Folgen für die Verfügbarkeit von Komponenten, die Geschwindigkeit des Netzausbaus sowie für Wettbewerb und Kostenstruktur, mit unmittelbaren Auswirkungen auf die Endverbraucherinnen.

Sicherheit und geografische Herkunft einzelner Lieferanten

Der VAT teilt ausdrücklich die Auffassung, dass Cybersicherheitsrisiken konsequent identifiziert und wirksam gemanagt werden müssen. Sicherheit darf jedoch nicht primär an der geografischen Herkunft eines Herstellers oder an politischen Zuschreibungen festgemacht werden, sondern muss sich an konkreten technischen, organisatorischen und betrieblichen Risikofaktoren orientieren.

Telekommunikationsunternehmen unterliegen bereits heute strengen gesetzlichen Vorgaben, insbesondere im Rahmen des Telekommunikationsrechts und der Umsetzung der NIS-2-Richtlinie. Sie sind verpflichtet, die Integrität, Verfügbarkeit und Vertraulichkeit ihrer Netze sicherzustellen und Risiken in ihren Lieferketten laufend zu bewerten und zu minimieren. Dieses bestehende Sicherheitsniveau ist bereits hoch entwickelt und hat sich in der Praxis bewährt. Zusätzliche regulatorische Eingriffe dürfen daher nicht zu einer Doppelregulierung führen oder die bewährte Betreiberverantwortung untergraben.

Keine zusätzliche Sicherheit durch ECCF-Zertifizierung interner Eigenentwicklungen

Ergänzend ist darauf hinzuweisen, dass viele Telekommunikationsunternehmen aufgrund der hohen technischen Komplexität ihrer Netze Softwarelösungen ausschließlich für den internen Gebrauch entwickeln, etwa für Monitoring-, Management- oder Orchestrierungszwecke. Diese Eigenentwicklungen entstehen innerhalb bereits streng regulierter und häufig nach ISO 27001 zertifizierter Unternehmen.

Eine zusätzliche Zertifizierung solcher nicht in Verkehr gebrachten internen Lösungen im Rahmen des ECCF (European Cybersecurity Certification Framework) würde keinen erkennbaren Sicherheitsgewinn bewirken. Sie würde vielmehr zu einer unverhältnismäßigen Doppel- bzw. Mehrfachbelastung der Unternehmen führen, da die betreffenden Organisationen bereits umfassenden gesetzlichen Anforderungen, insbesondere nach NIS-2, unterliegen und mit der im Cyber Security Act 2 vorgesehenen Cyber-Posture-Zertifizierung ohnehin einer externen, unabhängigen Gesamtbewertung ihrer Sicherheitsstrukturen unterzogen werden.

Conclusio

Zusammenfassend unterstützt der VAT das Ziel einer hohen Cybersicherheit in Europa. Dieses Ziel darf jedoch nicht zulasten der bestehenden digitalen Infrastruktur, der Versorgungssicherheit und der Wettbewerbsfähigkeit der Telekommunikationsbranche erreicht werden. Der Cyber Security Act 2 sollte daher so ausgestaltet werden, dass Sicherheit durch technische Exzellenz, transparente Verfahren und verantwortungsvolle Betreiberpflichten gewährleistet wird, nicht durch pauschale oder politisch motivierte Ausschlüsse von Herstellern.