



Digitalisierung, Regulierung

Cybersicherheit ohne *Regulierungsillusionen*

22.01.2026

Auf einen Blick

- Nach Jahren regulatorischer Verdichtung setzt die EU vermehrt auf Vereinfachung, Harmonisierung und Investitionssicherheit statt auf immer neue Detailregeln.
- Marktgetriebene Massnahmen, internationale Standards und technologische Expertise tragen mehr zur Resilienz bei als zunehmend kleinteilige staatliche Vorgaben.
- Die Schweiz ist im Cyberbereich bisher mit Augenmass gefahren – entscheidend ist nun, diesen Ansatz nicht aufzugeben und keine Regulierungen zu übernehmen, die die EU selbst bereits zu korrigieren beginnt.

Die Europäische Union schlägt in der Digitalpolitik ein neues Kapitel auf. Nach Jahren regulatorischer Verdichtung, mehren sich die Zeichen einer

Kurskorrektur. Der Digitale Omnibus, der angekündigte Digital Networks Act, die Revision des Cyber Security Act sowie der laufende digitale Fitnesscheck stehen für einen klaren Trend: Vereinfachung, Harmonisierung und ein stärkerer Fokus auf Investitionen und Umsetzung statt immer neuer Detailregeln.

Was die EU jetzt erkennt – und die Schweiz daraus lernen sollte

Ein zentrales Zerrbild prägt bis heute viele Debatten: Cybersicherheit entstehe nur, wenn der Staat Unternehmen zum Handeln zwingt. Freiwillige Massnahmen und Marktmechanismen würden nicht ausreichen. Die Praxis zeigt jedoch ein anderes Bild.

Cybersicherheit ist für Unternehmen kein Nice-to-have, sondern ein existenzieller Faktor. Datenverluste, Produktionsstopps oder Reputationsschäden haben direkte wirtschaftliche Konsequenzen. Wie stark und frühzeitig in Cybersicherheit investiert wird, unterscheidet sich jedoch deutlich nach Unternehmensgrösse.

Gerade KMU stehen bereits unter erheblichem Kosten und Bürokratie-Druck. Ihnen fehlen oft die finanziellen Spielräume, um komplexe regulatorische Vorgaben in der Cybersicherheit frühzeitig umzusetzen. Zusätzliche Detailregulierung hilft hier kaum weiter. Wirksamer sind Sensibilisierung, Orientierung und einfach zugängliche Informationen, die es ermöglichen, Risiken verhältnismässig und schrittweise zu managen. Zusätzlich gehen internationale Standards und Zertifizierungen wie ISO 27001 oder NIST-Frameworks oft weit über gesetzliche Minimalanforderungen hinaus.

Hinzu kommt, dass moderne Cloud und Sicherheitsanbieter globale Security Operation Center betreiben und Milliarden in Angriffserkennung, Redundanz und Automatisierung investieren. Dieses Sicherheitsniveau entsteht durch Nähe zur Technik und schnelle Anpassungsfähigkeit – nicht durch administrative Vorgaben im Jahresrhythmus.

Das bedeutet nicht, dass der Staat keine Rolle spielt. Er ist dort gefragt, wo Marktmechanismen an Grenzen stossen: bei Mindeststandards für kritische Infrastrukturen, bei klaren Verantwortlichkeiten und bei Transparenz. Was er

jedoch nicht leisten kann, ist operative Cybersicherheit im Alltag. Bedrohungen entwickeln sich schneller als Regulierung.

Genau hier setzt der europäische Kurswechsel an. Der Cyber Resilience Act illustriert die Lernkurve der EU besonders deutlich. Als komplexer und bürokratischer Eingriff in den Produktlebenszyklus wurde er von der Wirtschaft scharf kritisiert. Dass die EU diese Einwände nun aufnimmt, ist weniger ein Erfolg des Instruments als ein Eingeständnis, dass überladene Regulierung zum Standortnachteil wird.

Ein veritabler Paradigmenwechsel

Es geht nicht um Deregulierung, sondern um Standortpolitik. Sicherheit entsteht durch Verlässlichkeit, nicht durch immer neue Pflichten. Investitionen in Cybersicherheit erfolgen dort, wo Unternehmen wissen, woran sie sind.

Das Umdenken in der EU in Bezug auf Regulierung im digitalen Raum ist ein Warnsignal – nicht wegen eines heutigen Schweizer Alleingangs, sondern als Erinnerung, den bisherigen Kurs nicht aufzugeben. Im Cyberbereich hat die Schweiz gut daran getan, nicht vorzupreschen und europäische Vorgaben mit Augenmass umzusetzen. Entscheidend ist nun, nicht jene regulatorischen Altlasten zu übernehmen, die die EU selbst als zu komplex erkannt und zu korrigieren begonnen hat.

Nachhaltige Cybersicherheit entsteht dort, wo Unternehmen Verantwortung übernehmen – unterstützt, aber nicht ersetzt durch klare, einfache staatliche Leitplanken. Die EU beginnt, diese Erkenntnis umzusetzen. Die Schweiz sollte genau hinschauen.



Angela Anthamatten

Stv. Bereichsleiterin Wettbewerb & Regulatorisches



David Stauffacher

Projektleiter Infrastruktur und Digitales

© economiesuisse | www.economiesuisse.ch