Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

24.3810 Mo. SiK-S. Durchführung dringend notwendiger Cybersicherheitsprüfungen

Empfehlung: Ablehnung (Eventualiter: zwingend notwendige Präzisierungen im Zweitrat vornehmen)

Cybersicherheit hat für die ICT- und Internetbranche höchsten Stellenwert. Die Anbieter und Betreiber von digitalen Lösungen und Systemen, wie Geräten und Anwendungen, haben mit Blick auf ihre gesellschaftliche Verantwortung und ihren nachhaltigen wirtschaftlichen Erfolg (bspw. Reputation und drohende Konventionalstrafen) allergrösstes Interesse daran, sichere Produkte und Dienstleistungen anzubieten bzw. sichere Systeme zu betreiben. Darüber hinaus kommen sie bereits heute zahlreichen Pflichten im Bereich der Informations- und Cybersecurity nach, bspw. im Rahmen des Datenschutzgesetzes (DSG), Fernmeldegesetzes (FMG), Informationssicherheitsgesetzes (ISG) sowie deren Ausführungsverordnungen, als auch im Bereich der öffentlichen Beschaffung (siehe z.B. die «Mustervertragsklausel der BKB betreffend Cyberangriffen» - Link).

Die ICT- und Internetbranche bekennt sich zum Ziel, die Cybersicherheit der Schweiz weiter zu stärken. Das Testen von vernetzten Geräten und Anwendungen, wie es die Motion verlangt, kann eine mögliche Massnahme darstellen. Aus Sicht von Swico lässt die Motion jedoch zentrale Fragen hinsichtlich einer möglichen Umsetzung offen:

- **Test-Umfang**: Dieser muss klar eingegrenzt werden. Die Umschreibung «vernetzte Infrastrukturen, Geräte und Anwendungen» ist zu allgemein gefasst, sodass praktisch alle IT-Produkte in der Schweiz angesprochen wären. Auch der Begriff «Lücken» wird nicht näher spezifiziert. Diese Begriffe müssen sinnvoll definiert und der Test-Umfang entsprechend eingegrenzt werden. In erster Linie sind bestehende Gesetze anzuwenden. Neue «Test-Pflichten» sind potenziell nur dort angezeigt, wo mit Tests auf wirtschaftliche Weise ein Mehrwert geschaffen wird, bspw. bei Geräten und Anwendungen, die noch nicht über angemessene Zertifikate verfügen, wo effektiv massgebliche Risiken bestehen und ein klares Ownership bzw. Verantwortlichkeiten fehlen.
- **Harmonisierung**: Cybersicherheit und «digitale Souveränität», wie in der Motion erwähnt, sind nicht mit isolierten Massnahmen zu erzielen. Cybersicherheit hört nicht an der Landesgrenze auf, sondern ist ein globales Thema. Bezüglich allfälliger Testpflichten und -standards sowie der notwendigen Anerkennung von bestehenden Zertifikaten (siehe oben), ist eine enge Abstimmung bzw. Harmonisierung mit anerkannten internationalen Standards, bspw. dem Cyber Resilience Act der EU, notwendig, ohne der Wirtschaft über den Test-Aspekt hinausgehende Pflichten aufzuerlegen. Multiple Test- und Nachweispflichten sind unbedingt zu verhindern.
- **Bürokratie**: Den Anbietern und Betreibern von digitalen Lösungen, welche sich bereits an bestehende Pflichten halten und für ihre Geräte und Anwendungen anerkannte Zertifikate vorweisen können, sogenannte «good actors», darf kein zusätzlicher bürokratischer Aufwand erwachsen.
- **Finanzierung**: Auch die Finanzierungsfrage lässt die Motion offen. Für Swico ist klar, dass den erwähnten «good actors» keine finanziellen Verpflichtungen erwachsen dürfen. Auch einer staatlichen Finanzierung stehen wir kritisch gegenüber.

Angesichts dieser bedeutenden Unklarheiten empfehlen wir, die Motion abzulehnen. Sollte der Ständerat die Motion annehmen, fordern wir zwingend eine konkrete Auslegeordnung bezüglich der Bedrohungslage und Vornehmen der notwendigen Präzisierungen (siehe oben) nach Anhörung der betroffenen Anspruchsgruppen im Zweitrat bzw. in der SiK-N. Als Wirtschaftsverband der Anbieter von digitalen Geräten und Anwendungen steht Swico für entsprechende Hearings selbstverständlich zur Verfügung.