economiesuisse

Cybersicherheit: Kooperation schlägt staatlichen Zwang

Staatlicher Zwang und Überregulierung sind meistens kontraproduktiv, gerade in einem Bereich wie der Cybersicherheit, in dem alle Akteure dasselbe Ziel verfolgen. Es braucht Zusammenarbeit und praxisnahe Lösungen. Das Thema ist ein Gebot der Stunde, das hat die Bundespolitik zuletzt mit der Verschärfung des Informationssicherheitsgesetzes (ISG) gezeigt. Auch die Wirtschaft unterstützt – nur schon aus Eigeninteresse – ein starkes Augenmerk auf die Cybersicherheit.

Bei der Cybersicherheit verfolgen alle Beteiligten aus Politik, Wirtschaft und Gesellschaft ein gemeinsames Interesse: den Schutz sensibler Daten und kritischer Infrastrukturen. Trotz dieser harmonischen Ausgangslage setzt die Bundespolitik vermehrt auf staatliche Regulierung und Zwangsmassnahmen, wie zuletzt bei der Verschärfung des Informationssicherheitsgesetzes (ISG). Das Vertrauen in die Schweizer Unternehmen scheint gering. Die Einführung eines staatlich verordneten "Zwangsprogramms" ist gerade in diesem Bereich aber keine gute Idee und weder zielführend noch effizient. Der Weg zu mehr Sicherheit führt nicht über mehr Detailregulierung und darf auch nicht «gegen» die Unternehmen beschritten werden. Auch zusätzliche Massnahmen "mit dem Vorschlaghammer", wie sie im Rahmen der Motion 24.3810 aktuell diskutiert werden, sind vor diesem Hintergrund eher schädlich als nützlich.

«Statt auf Zwang zu setzen, sollte die Politik auf Kooperation bauen.»

Bereits die Revision des ISG und nun auch der Entwurf der geplanten Cybersicherheitsverordnung haben gezeigt, dass der Staat in diesem hochsensiblen Bereich ständig in ein Rollenverständnis verfällt, das der Sache mehr schadet als nützt. Einerseits zieht er mit Zwangsmassnahmen eine Verantwortung an sich, die er gar nicht übernehmen kann, andererseits schafft er unnötigen Hürde für Unternehmen, die bereits aktiv in ihre Sicherheit investieren. Drittens hemmt er damit eine gesunde Fehlerkultur. Statt auf Zwang zu setzen, sollte die Politik einen kooperativen Ansatz verfolgen, bei dem alle Akteure ihre Expertise und Ressourcen einbringen können.

Es wäre wenig sinnvoll, wenn die Polizei die Stärke der Fahrradschlösser (auf Kosten der Velobesitzer) an den Veloständern überprüft und diejenigen, die vermeintlich zu schwache Schlösser verwenden, bestraft. Stattdessen sollte es darum gehen, klar zu kommunizieren, welche Schlösser welche

Sicherheitsvorteile bieten. Die Verantwortung bleibt bei der Besitzerin, die selbst entscheidet, welche Massnahmen für sie sinnvoll sind. Genauso verhält es sich auch bei der Cybersicherheit: Zwang und Strafen allein helfen nicht weiter. Wichtiger ist, dass Unternehmen wissen, welche Massnahmen wirklich effektiv sind, um ihre Systeme zu schützen.

Das Ziel sollte sein, einen sicheren Rahmen zu schaffen, der auf Vertrauen, Kooperation und praktikablen Massnahmen beruht. Denn Cybersicherheit kann nicht mit einer «Vollkasko»-Mentalität erreicht werden, bei der jede Lücke durch staatliche Kontrolle geschlossen werden soll. Stattdessen ist ein ausgewogenes Schlüsselsystem notwendig – wie im Alltag, wo wir unsere Häuser sichern, ohne sie komplettt zu verbarrikadieren. Nur so kann eine effiziente und nachhaltige Sicherheitsstrategie gelingen.

Der technologische Fortschritt in der Cybersicherheit ist rasant, und neue Lösungen entstehen durch Wettbewerb und kreative Innovation. Staatliche Überregulierung könnte diese Entwicklung hemmen und den Markt in seiner Anpassungsfähigkeit einschränken. Cybersicherheit ist kein Selbstzweck und auch kein Thema, das sich mit immer mehr Paragraphen lösen lässt. Das geht nur mit Praxisnähe, Kooperation und Pragmatismus.