



Positionspapier zum regulatorischen Umgang mit Cyberrisiken

Das Wichtigste in Kürze:

- Cyberangriffe entwickeln sich ständig weiter, wodurch Unternehmen unter hohem Druck stehen, Sicherheitslücken schnell zu erkennen, zu priorisieren und wirksam zu beheben.
- Ein fundiertes Verständnis der aktuellen Bedrohungslage ist entscheidend, um die Kommunikations- und Informationsinfrastrukturen wirksam zu schützen.
- Cyberrisiken erfordern gemeinsames Handeln, wobei die Wirtschaft Verantwortung übernimmt und klare Rahmenbedingungen vom Staat erwartet.

Cyberangriffe nehmen weltweit zu und stellen eine zunehmende Bedrohung für Wirtschaft, Staat und Gesellschaft dar. Betroffen sind nicht nur kritische Infrastrukturen sondern Unternehmen aller Grössen. Dies zeigt, die Bekämpfung von Cyberrisiken ist eine gesamtgesellschaftliche Aufgabe.

Positionspapier zeigt Weg für verlässlichen Rahmen auf

Trotz dieser wechselseitigen Ausgangslage setzte die Bundespolitik auf staatliche Regulierung und Zwangsmassnahmen statt auf Zusammenarbeit. Dies zeigte sich zuletzt bei der Verschärfung des Informationssicherheitsgesetzes (ISG), welches am 1. April 2025 in Kraft getreten ist. Strenge Meldepflichten werden dort mit

strengen Strafen durchgesetzt. Das Unternehmen, das von einem Cyberangriff betroffen ist, wird damit gleich mehrfach bestraft.

Dabei geht es auch anders: die Wirtschaft ist bereit, Verantwortung zu übernehmen, dabei erwartet sie vom Staat jedoch einen verlässlichen Rahmen, der auf Vertrauen, Flexibilität und gemeinsamer Verantwortung basiert.

Vor diesem Hintergrund hat economiesuisse ein Positionspapier zum regulatorischen Umgang mit Cyber-Risiken veröffentlicht, das mit den Mitgliedern eng abgestimmt ist.

Zum Positionspapier

Cybersicherheit braucht einen flexiblen und wirksamen Regulierungsansatz

Cyber Risiken lassen sich nicht durch starre Vorschriften regeln. Vielmehr braucht es einen dynamischen, prinzipienbasierten Regulierungsrahmen, der Innovationen nicht hemmt und eine schnelle Reaktion auf neue Bedrohungen ermöglicht. Die Schweizer Wirtschaft spricht sich daher für folgende Grundsätze aus:

- **Kooperation auf Augenhöhe zwischen Staat und Wirtschaft:** Die Verantwortung für Cybersicherheit ist gemeinsam zu tragen. Notwendig ist ein vertrauensvoller, kontinuierlicher Dialog.
- **Stärkung branchenspezifischer Selbstregulierung:** Bewährte Branchenlösungen erhöhen die Wirksamkeit und Flexibilität im Umgang mit Risiken.
- **Verlässliche Datenbasis und Informationsaustausch:** Ein gemeinsames Lagebild und der Austausch anonymisierter Bedrohungsinformationen sind zentral.
- **Förderung statt Sanktionierung:** Prävention und Sicherheitsmassnahmen sollen durch positive Anreize und Unterstützung gefördert werden – nicht durch übermässige Sanktionen.

Standortvorteil durch resiliente digitale Infrastruktur

Ein effektiver Schutz vor Cyber Risiken stärkt die digitale Souveränität der Schweiz und ist ein zentraler Standortfaktor. Nur durch innovationsfreundliche Rahmenbedingungen kann die Wettbewerbsfähigkeit der Schweizer Wirtschaft langfristig gesichert werden.

Das Positionspapier soll einen Beitrag zur breiten Diskussion über den regulatorischen Umgang mit Cyber-Risiken leisten und dabei wichtige Impulse für die zukünftige Ausgestaltung eines wirksamen, innovationsfreundlichen und standortgerechten Regelwerks liefern.