Sachdokumentation:

Signatur: DS 5228

Permalink: www.sachdokumentation.ch/bestand/ds/5228

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

economiesuisse

→ Positionspapier zum regulatorischen Umgang mit Cyberrisiken

DIE SCHWEIZ STEHT VOR EINER ZUNEHMENDEN VIELFALT HOCHENTWICKELTER CYBERBEDROHUNGEN. RANSOMWARE-ANGRIFFE AUF MITTELSTÄNDISCHE UNTERNEHMEN UND GROSSKONZERNE VERURSACHEN JEDES JAHR ERHEBLICHE SCHÄDEN UND KÖNNEN GANZE PRODUKTIONSKETTEN LAHMLEGEN. BESONDERS KRITISCHE INFRASTRUKTUREN – VON ENERGIEVERSORGERN ÜBER GESUNDHEITSEINRICHTUNGEN BIS HIN ZU VERKEHRSSYSTEMEN – GERATEN INS VISIER KRIMINELLER GRUPPEN, DIE GEZIELT SCHWACHSTELLEN AUSNUTZEN, UM DIE VERSORGUNGSSICHERHEIT UND ÖFFENTLICHE ORDNUNG ZU GEFÄHRDEN.

Ausgangslage

- → Cyberangriffe entwickeln sich stetig weiter. Die Angreifer passen ihre Methoden – etwa bei Ransomware, Phishing und anderen Angriffen – kontinuierlich an. Durch den Einsatz neuer Technologien und automatisierter Werkzeuge verkürzt sich die Zeitspanne, in der Unternehmen Sicherheitslücken erkennen und schliessen können, zunehmend. Daraus ergibt sich ein hoher Handlungsdruck: Schwachstellen müssen schnell identifiziert, priorisiert und wirksam behoben werden, bevor sie ausgenutzt werden.[1]

- → Ein tiefgreifendes Verständnis der aktuellen Bedrohungslage ist unerlässlich. Nur mit fundierten Kenntnissen über Cyberrisiken lassen sich die Kommunikations- und Informationsinfrastrukturen in der Schweiz und darüber hinaus wirksam schützen.[2]

- → Der Umgang mit Cyberbedrohungen erfordert gemeinsames, angemessenes Handeln. Die Bekämpfung von Cyberrisiken ist eine gesamtgesellschaftliche Aufgabe. Die Wirtschaft ist bereit, Verantwortung zu übernehmen – erwartet vom Staat jedoch einen verlässlichen Rahmen, der auf Vertrauen, Flexibilität und gemeinsamer Verantwortung basiert.

KONTAKT

ERICH HERZOG
Mitglied der Geschäftsleitung, Bereichsleiter Wettbewerb & Regulatorisches
erich.herzog@economiesuisse.ch

ANGELA ANTHAMATTEN
Stv. Bereichsleiterin
Wettbewerb & Regulatorisches
angela.anthamatten@economiesuisse.ch

1 Siehe auch BACS – Cybersicherheit – Lage in der Schweiz und international, Halbjahresbericht 2024/II (Juli – Dezember), S. 7 ff. [zit. «BACS»].
2 BACS, S. 5.

Miteinander statt Misstrauen

Eine widerstandsfähige digitale Wirtschaft braucht eine enge, gleichberechtigte Partnerschaft zwischen Staat und Wirtschaft. Angesichts zunehmend komplexer und dynamischer Cyberbedrohungen greifen starre, technikferne Regulierungsansätze zu kurz. Stattdessen sind flexible gesetzliche Rahmenbedingungen erforderlich, die es Unternehmen ermöglichen, rasch und wirksam auf neue Bedrohungen zu reagieren. Diese Flexibilität sollte durch branchenspezifische Selbstregulierung und praxisnahe Empfehlungen ergänzt werden, um Innovationsfähigkeit und Sicherheitsstandards langfristig zu sichern.

Die Position der Wirtschaft

- **Partnerschaft auf Augenhöhe mit dem Staat:** Die Zusammenarbeit muss auf gegenseitigem Vertrauen, einer konstruktiven Fehlerkultur und der gezielten Nutzung gemeinsamer Stärken basieren. Der Staat soll nicht als Kontrollinstanz auftreten, sondern als aktiver Partner in der gemeinsamen Verantwortung für Cybersicherheit.

- **Effizienter und ausgewogener Regulierungsrahmen statt einseitiger Lastenverteilung:** Unternehmen brauchen Schutz vor Cyberrisiken – ohne dass ihnen allein die Verantwortung aufgebürdet oder ihre Innovationsfähigkeit durch überzogene Vorgaben eingeschränkt wird. Es braucht einen fairen, praxistauglichen Regulierungsrahmen.

Die dynamische Bedrohungslage erfordert eine adaptive Regulierung. Im Fokus stehen:

- **Prinzipienbasierte Leitplanken statt starrer Vorschriften:** Starre gesetzliche Regelungen greifen bei der Bewältigung von Cyberrisiken zu kurz. Gefragt ist ein kooperativer Ansatz, der auf Flexibilität, Eigenverantwortung und gegenseitigem Vertrauen basiert.

- **Branchenspezifische Selbstregulierung stärken:** Sie ist zentral, um Flexibilität, Agilität und damit wirksame Cybersicherheit zu ermöglichen. Der Staat sollte bestehende Strukturen anerkennen, fördern und systematisch in den regulatorischen Rahmen einbinden.

- **Verlässliche Datenbasis und gegenseitiger Informationsaustausch:** Für Staat und Wirtschaft ist ein gemeinsames Lagebild zentral. Ein wirksamer Schutz vor Cyberbedrohungen erfordert einen kontinuierlichen, bidirektionalen Informationsfluss – insbesondere durch die Bereitstellung aggregierter oder anonymisierter Daten durch staatliche Stellen.

- **Anreize statt Sanktionen – Verantwortung stärken, nicht abschrecken:** Eine konstruktive Sicherheitskultur entsteht nur, wenn Unternehmen ohne Angst vor unverhältnismässigen Konsequenzen agieren können. Verwaltungs- oder strafrechtliche Sanktionen sollten auf vorsätzliches Fehlverhalten beschränkt bleiben – nur so lässt sich eine offene und lernbereite Fehlerkultur fördern.

Besonderheiten bei der Regulierung von Cyberrisiken

- Cyberrisiken lassen sich nicht einfach wegregulieren: Kein Unternehmen strebt einen Cybervorfall an – das macht Prävention zu einem natürlichen Eigeninteresse der Wirtschaft. Umso wichtiger ist es, regulatorisch auch präventive Massnahmen systematisch zu fördern und anzuerkennen.

- Fixe Sicherheitsvorgaben sind der Realität nicht gewachsen: Die Bedrohungslage verändert sich ständig und in hoher Geschwindigkeit. Regulierungen müssen diesem Wandel gerecht werden – durch adaptive, technologieoffene Ansätze statt starrer Regeln.

- Zu engmaschige Regulierung schafft neue Risiken: Zwar kann sie kurzfristig formale Rechtssicherheit aus Compliance-Sicht bieten, doch behindert sie gleichzeitig Innovationsprozesse und die agile Weiterentwicklung von Abwehrmassnahmen gegen Cyberbedrohungen. Starre Vorgaben dürfen nicht zum Sicherheitsrisiko werden.

Gesetzgebungen müssen:

- flexibel und zukunftsgerichtet sein, damit Unternehmen auf neue Bedrohungen eingehen und bei technologischen Fortschritten adäquat reagieren können (z.B. Entwicklungen rund um KI und Quantentechnologie), ohne in Gefahr zu laufen, gegen geltendes Recht zu verstossen.

- sich auf allgemeine, prinzipienbasierte Regelungen beschränken, wobei Selbstregulierung und Branchenempfehlungen dies ergänzen, um die notwendige Agilität zu erhalten.

Staatliche Unterstützung ausbauen – statt Überwachung auszuweiten

Der Staat muss:

- technische Ressourcen gezielt stärken, denn ein wirksamer Schutz vor Cyberbedrohungen setzt ein belastbares, staatlich unterstütztes Frühwarnsystem voraus. Dafür müssen ausreichend technische und personelle Ressourcen bereitgestellt werden.

- eine enge Partnerschaft mit der Wirtschaft fördern, da ein kontinuierlicher, vertrauensvoller Dialog zwischen Staat und Unternehmen entscheidend ist, um Cyberrisiken wirksam zu erkennen, einzuordnen und gemeinsam zu bewältigen.

Diese Zusammenarbeit ermöglicht:

- die Entwicklung gemeinsamer Sicherheitsstandards, da staatliches Wissen mit unternehmerischer Praxis kombiniert wird und so effektive und praxisnahe Standards entstehen.

- einen intensivierten Informationsaustausch, bei dem der zeitnahe und umfassende Austausch von Informationen über die Bedrohungslage und Vorfälle entscheidend ist. Dies gilt insbesondere für den Staat, der der Wirtschaft solche Informationen in aggregierter oder anonymisierter Form zur Verfügung stellen muss. Staatliche Unterstützung in Form von Schulungen und Informationsplattformen stärkt die Cybersecurity-Fähigkeiten der Unternehmen weiter.

- den Austausch von Best Practices, denn ein kontinuierlicher Dialog fördert den Austausch bewährter Verfahren und innovativer Lösungen zur Cyberabwehr.

- eine schnelle Reaktionsfähigkeit, da gemeinsame Arbeitsgruppen und Kommissionen schnelle Anpassungen an neue Bedrohungen und technologische Entwicklungen ermöglichen.

- die Förderung von Public-private-Partnerships (PPP), wodurch gemeinsame Projekte die Entwicklung und Implementierung fortschrittlicher Sicherheitslösungen vorantreiben.