Wie die Schweiz ihre digitale Resilienz erhöhen kann

Erkenntnisse der ersten “Blind Spots”-Veranstaltung zum Thema Cybersicherheit

Juni 2025

Zusammenfassung:

Die Veranstaltungsreihe "Blind Spots" bringt Expert:innen aus Wissenschaft, Wirtschaft und Gesellschaft sowie Politik und Verwaltung in einen Dialog, um mögliche Krisensituationen in der Schweiz zu diskutieren und blinde Flecken im aktuellen Wissensstand zu identifizieren. Träger der Reihe sind die Stiftung Mercator Schweiz, der ETH-Rat und economiesuisse. Ziel ist der offene Austausch zur Stärkung des gegenseitigen Vertrauens und zur Krisenvorbereitung. Die erste Veranstaltung zum Thema Cybersicherheit fand im April 2025 in Zürich statt.

Zentrale Erkenntnisse der Expert:innen sind:

- *Eine effiziente Zusammenarbeit zwischen Wissenschaft, Wirtschaft, Politik/Verwaltung und Gesellschaft im Krisenfall erfordert vorgängig geklärte Rollen und Abläufe.*
- *Resilienz ist kein Modewort, sondern eine strukturelle Notwendigkeit für die Schweiz, vor allem in Hinblick auf Lieferketten und technologische Souveränität.*
- *Die Schweizer Forschung verfügt über ein hohes Fachwissen, der Transfer in die praktische Anwendung aber könnte verbessert werden.*
- *Es bestehen wirtschaftliche Systemrisiken durch Anbieter-Abhängigkeit und Vernachlässigung von KMUs sowie fehlende Marktanreize für Cybersicherheit. Compliance bleibt oft der einzige Hebel.*
- *Die Vorbereitung der breiten Bevölkerung auf Cyberbedrohungen hat noch viel Entwicklungspotenzial.*
- *Internationale Kooperation, offene Protokolle und Public-Private-Partnerships könnten die digitale Sicherheit in der Schweiz erhöhen.*

BLIND SPOTS

Ausgangslage

"Blind Spots" ist eine Veranstaltungsreihe mit Fokus auf gegenwärtige und zukünftige Krisensituationen. Die Serie wurde von der Stiftung Mercator Schweiz, Economiesuisse und dem ETH-Rat ins Leben gerufen, um eine offene, strukturierte Diskussion zwischen Wissenschaft, Wirtschaft und Gesellschaft zu fördern – und zwar vor dem Ernstfall. Die Auswahl der Themen orientiert sich an den Vorgaben des Bundesrates.

Die erste Ausgabe von “Blind Spots” fand am 9. April 2025 in Zürich statt und versammelte rund 70 Expertinnen und Experten aus Wissenschaft, Wirtschaft und Gesellschaft sowie Verwaltung. Sie widmete sich der Frage, wie verschiedene Akteur:innen der Schweiz sich für Bedrohungen im Bereich Cybersicherheit rüsten können. Im Zentrum stand der Aufbau kollektiver Krisenkompetenz: Wie kann ein gemeinsames Verständnis von Krisen im Cyberbereich entstehen, das praxisrelevant und zukunftsgerichtet ist? Mit welchen Herausforderungen sind Unternehmen, Politik/Verwaltung und Öffentlichkeit im Bereich Cybersicherheit konfrontiert? Wie verändern sich diese Herausforderungen in den kommenden 5-10 Jahren? Wie gut ist die Schweiz auf diese Herausforderungen vorbereitet? Wie liesse sich die Resilienz der verschiedenen Akteur:innen erhöhen? Welche technologischen Abhängigkeiten bestehen?

Diese zentralen Herausforderungen wurden von Vertreter:innen von Wissenschaft, Wirtschaft und Gesellschaft diskutiert und live bewertet. Eine vor Ort erstellte Umfrage nutzte eine Skala von 1 (stimme gar nicht zu) bis 5 (stimme voll zu). Die Ergebnisse und Diskussionen zeigen Handlungsbedarf für Politik, Wissenschaft und Wirtschaft.

Resilienz, Governance und Offenheit

Mit nur 2.76 Punkten wurde die gegenwärtige Zusammenarbeit zwischen Wissenschaft, Wirtschaft und Gesellschaft sowie Politik und Verwaltung sehr kritisch bewertet. Der Ruf nach Sortierungsarbeit vor der Krise war demnach laut (4.07). Wer macht was im Krisenfall? Der gezielte Blick auf strategisch wichtige Lieferketten wurde auch als dringlich anerkannt (4.27), ebenso wie der Abbau technologischer Abhängigkeiten (3.63). Resilienz wurde dabei als konkrete Herausforderung deutlich. Fehlende Redundanzen, mangelnde Abstimmungen und historisch gewachsene Abhängigkeiten machen die Schweiz zurzeit höchst verletzlich. Offenheit wurde dabei unter anderem als Bedingung genannt: Mit Public-Private-Partnerships, offenen Protokollen und internationalem Austausch könne Cybersicherheit in einer vernetzten Welt gelingen (4.07 Punkte).

Wissenschaft zwischen Erkenntnis und Umsetzung

Aus wissenschaftlicher Sicht verfüge die Schweiz gemäss Expert:innen über gutes Fachwissen, doch die Umsetzung in die Praxis bleibe eine Herausforderung. Das zeigte sich auch im Umfrageresultat. So wurde die Wissenschaft als gut informiert über zukünftige Krisen (3.56) eingeschätzt. Gleichzeitig bestanden Zweifel daran, dass Cyberprobleme mit noch komplexeren IT-Systemen angegangen werden könnten (2.38 Punkte). Die sozialen und organisationellen Faktoren spielen gemäss Expert:innen eine ebenso wichtige Rolle in der

Cyber-Resilienz. Die Wissenschaft forderte zudem mehr Übersetzung von Forschung in Governance, etwa durch formelle Codeverifikationen, automatisierte Tests und frühzeitige Einbindung von Securitykonzepten in die Informatikausbildung. Die Idee eines Schweizer Qualitätssiegels für Cybersicherheit, analog zur Schweizer Präzision in der Mechanik, fand Zustimmung (3.73).

Wirtschaftliche Investitionslücken und Systemrisiken

Die wirtschaftliche Perspektive offenbarte eine Mischung aus Systemrisiken und strukturellen Lücken. Besonders die Rolle grosser Tech-Anbieter wurde kritisch gesehen (4.07), ebenso wie die Vernachlässigung der KMUs (3.93). Die Marktdynamik schaffe keine ausreichenden Investitionsanreize für Cybersicherheit (3.48), und Compliance bleibe häufig der einzige aber äusserst wichtige Hebel. Die Wirtschaft forderte zudem eine stärkere Ausbildung von Entscheidungsträgerinnen (4.09), sowie die gezielte Förderung von Public-Private-Partnerships (3.93). Ein besonders hoher Wert (4.48) unterstrich, wie stark Cyberrisiken inzwischen die Digitalisierung der Wirtschaft beeinflussen.

Gesellschaftliche Beteiligung statt Ausschluss

Die grösste Baustelle offenbarte sich aber in der gesellschaftlichen Dimension. Mit nur 2.2 Punkten wurde die gegenwärtige Vorbereitung der breiten Bevölkerung auf Bedrohungen im Bereich Cybersicherheit sehr schlecht bewertet. Auch die Möglichkeiten gesellschaftlicher Partizipation, etwa über Open Source (2.92), wurden als unzureichend eingeschätzt. Die Diskussion hob hervor, dass Bürgerinnen und KMUs oft nicht über Ressourcen verfügten, um sich aktiv zu schützen. Nötig seien leicht zugängliche, geprüfte Open-Source-Tools, aber auch eine neue Fehlerkultur, die Betroffene nicht stigmatisiere. Der Fokus müsse auf systemischer Aufklärung, finanzieller Unterstützung zivilgesellschaftlicher Organisationen und Verbände, sowie strukturellem Empowerment liegen. Nur so könne die Schweiz in einer Welt individualisierter Bedrohungen das Vertrauen erhalten.

BLIND SPOTS

Handlungsempfehlungen

- **Resilienz als Langzeitstrategie verankern**: Anbieter-Abhängigkeiten und grenzübergreifende Lieferketten können nicht über Nacht aufgehoben werden. Eine gezielte Förderung nationaler Kompetenzen, etwa im Bereich spezialisierter Chips oder sicherheitszertifizierter Software, ist essenziell. Doch auch Diversifikation und Doppelungen von Lieferpartnerschaften sind eine Resilienzmöglichkeit, gerade im Bereich spezialisierter Chips.
- **Governance und Risikomanagement stärken**: Es braucht klare Definitionen des Krisenfalls. Zuständigkeiten und Abläufe müssen vor dem Krisenfall definiert und eingeübt werden. Operative Verwaltung, Forschung und Gesellschaft sollten schon heute gemeinsam belastbare Krisenstrukturen im Bereich Cybersicherheit entwickeln.
- **Talente sichern und Ausbildung fördern**: Die Schweiz muss ihre Informatik- und Securitykonzepte im dualen Bildungssystem verankern, um Fachkräfte auf allen Ebenen auszubilden, vom Techniker bis zur Verwaltungsrätin.
- **Offenheit statt Abschottung**: Eine resiliente Schweiz muss auf Kooperationen und offene Protokolle setzen, um Monokulturen zu vermeiden und Zugang zu interopearblen Best-of-Breed-Lösungen zu erhalten.
- **Gesellschaft einbinden**: Praktische, offene Tools und eine Fehlerkultur sind entscheidend, damit auch KMUs und Bürger:innen aktiv zur Cyberresilienz beitragen können.

BLIND SPOTS

Querschnittspanel

42

Der Dialog zwischen Wissenschaft, Wirtschaft und Gesellschaft funktioniert sehr gut.

2.76

Es braucht Sortierungsarbeit vor der Krise: Wer berät wen wann? Welche Expertise liegt in der Wissenschaft, Wirtschaft, Verwaltung?

4.07

Die Schweiz muss ihre Lieferketten besser untersuchen, um sich besser positionieren zu können.

4.27

Die Schweiz muss technologische Abhängigkeiten überwinden.

3.63

Die Schweiz muss an "gute Chips" kommen, um beim internationalen KI-Wettbewerb mitmachen zu können.

3.6

Cybersicherheit ist nur mit einer offenen Schweiz möglich.

4.07

Ich fand den ersten „Blind Spots“-Event nützlich und würde gerne wieder teilnehmen.

4.05

BLIND SPOTS

Panel: Gesellschaft

42

Die Schweizer Gesellschaft ist sehr gut auf Cybersicherheitbedrohungen vorbereitet.

2.2

Bürger und Bürgerinnen tragen in der Schweiz erheblich zum Problem Cybersicherheit bei.

3.03

"Open Source" ist eine Möglichkeit, die Gesellschaft in die Cybersicherheit einzubeziehen.

2.92

KI-Agenten sind ein grosser Blind Spot am Schweizer Cybersicherheitsorizont.

3.6

Das Thema Cybersicherheit muss auf einer grösseren und geopolitischeren Ebene angegangen werden.

4.07

BLIND SPOTS

Panel: Wirtschaft

45

Die Schweizer Wirtschaft hat erhebliche blinde Flecken im Bereich der Cybersicherheit.

3.35

"Grossfirmen wie Microsoft" stellen "Klumpenrisiken" für die Schweiz dar.

4.07

Die Vernachlässigung von KMUs bei der Finanzierung der Cybersicherheit ist ein blinder Fleck.

3.93

Die Wirtschaft muss stärker mit der Wissenschaft interagieren und sich mit ihr austauschen ("give and take").

3.5

Die Marktdynamik schafft keine ausreichenden Anreize für Investitionen in die Cybersicherheit.

3.48

Die Wirtschaft muss die konkreten Kosten einer Cybersicherheitskrise antizipieren und berechnen.

3.61

Die Auswirkungen der Cybersicherheit auf die Wirtschaft werden durch die Digitalisierung immer grösser.

4.48

Die Politik sollte öffentlich-private Partnerschaften stärker fördern (Public-Private-Partnerships).

3.93

EntscheidungsträgerInnen müssen im Bereich Cybersecurity besser ausgebildet werden.

4.09

BLIND SPOTS

Panel: Wissenschaft

52

Die Wissenschaft ist sehr gut über zukünftige Sicherheitskrisen informiert (no unknown unknowns).

3.56

Die Schweiz sollte mehr in Talente und Innovation in den Bereichen "Routing, Kryptologie, physische Infrastruktur" investieren.

3.96

Die Schweizer Wissenschaft sollte zu einem Gütesiegel für IT-Qualität werden.

3.73

Die "Komplexität der IT-Systeme" kann nur mit noch komplexeren IT-Systemen angegangen werden.

2.38

Der mangelnde Fokus auf die "Kette der Abhängigkeiten" ist ein blinder Fleck der aktuellen Forschung.

3.56