Grundlagenpapier – Innovate Switzerland

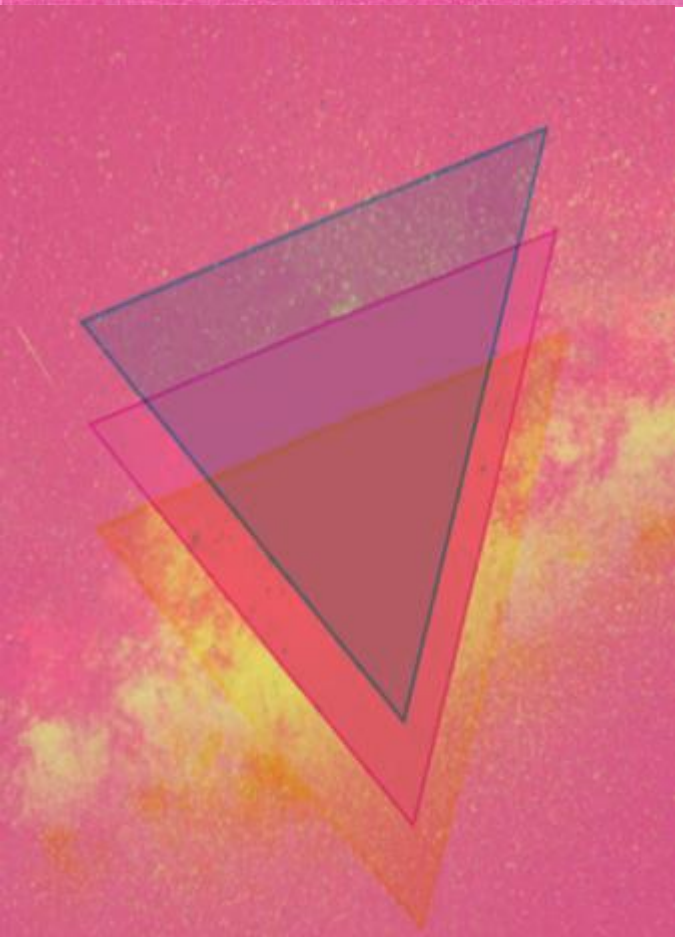
From Digital Sovereignty to Resilience

Wie Unternehmen im Zeitalter der digitalen Souveränität ihre Resilienz stärken.
Und warum ein neues Ökosystem die Grundlage der digitalen Schweiz bildet.

W.I.R.E.
WEB FOR INTERDISCIPLINARY RESEARCH AND EXPERTISE
THINK TANK FOR BUSINESS, SCIENCE AND SOCIETY

INNOVATE SWITZERLAND

Inhalt



Resilienz wird zur zentralen Voraussetzung für die digitale Transformation und echte Innovation.

Ausgangslage: Resilienz als strategischer Imperativ

Der Übergang in eine neue geopolitische Weltordnung, die durch eine Verschiebung des Zentrums der Weltwirtschaft in den pazifischen Raum und die Schwächung des transatlantischen Bündnisses geprägt ist, hat in Europa und in der Schweiz innert kurzer Zeit zu einer starken Sensibilisierung für digitale Souveränität geführt. Dies betrifft einerseits politische Forderungen nach Entkopplung und Unabhängigkeit in der Bereitstellung und Nutzung von digitalen Dienstleistungen, andererseits die erhöhte Sensibilisierung der Bevölkerung in Bezug auf die Privatheit und Sicherheit ihrer Daten.

Nachdem das Thema der digitalen Souveränität lange Zeit selbst bei IT-Verantwortlichen kaum als relevant angesehen wurde, hat die rückläufige Planungsunsicherheit, die Frage nach digitaler Unabhängigkeit in den Mittelpunkt der öffentlichen Debatte undder strategischen Ausrichtung von Unternehmen gerückt.

Aktuell werden in Europa und der Schweiz Initiativen und Lösungen diskutiert, die dem erwarteten Kontrollverlust über digitale Ressourcen und Prozesse entgegenwirken sollen. Während einzelne Meinungsträgerinnen die Lösung vor allem in der Entkopplung von ausländischen Anbietern und Infrastrukturen sehen, suchen Unternehmen vorwiegend nach pragmatischen Lösungen, die eine optimale Balance zwischen Innovationfähigkeit, Kontrolle und Kosten sicherstellen. In diesem Prozess ist eine unübersichtliche Situation entstanden, in der sich Bedenken und Optimismus im Spannungsfeld zwischen ideologischen und wirtschaftlichen Zielbildern bewegen.

Der Schweizer Bundesrat definiert Souveränität als staatliche Hoheit, in der Folge gilt es für Unternehmen die Grundlagen für Resilienz zu schaffen.

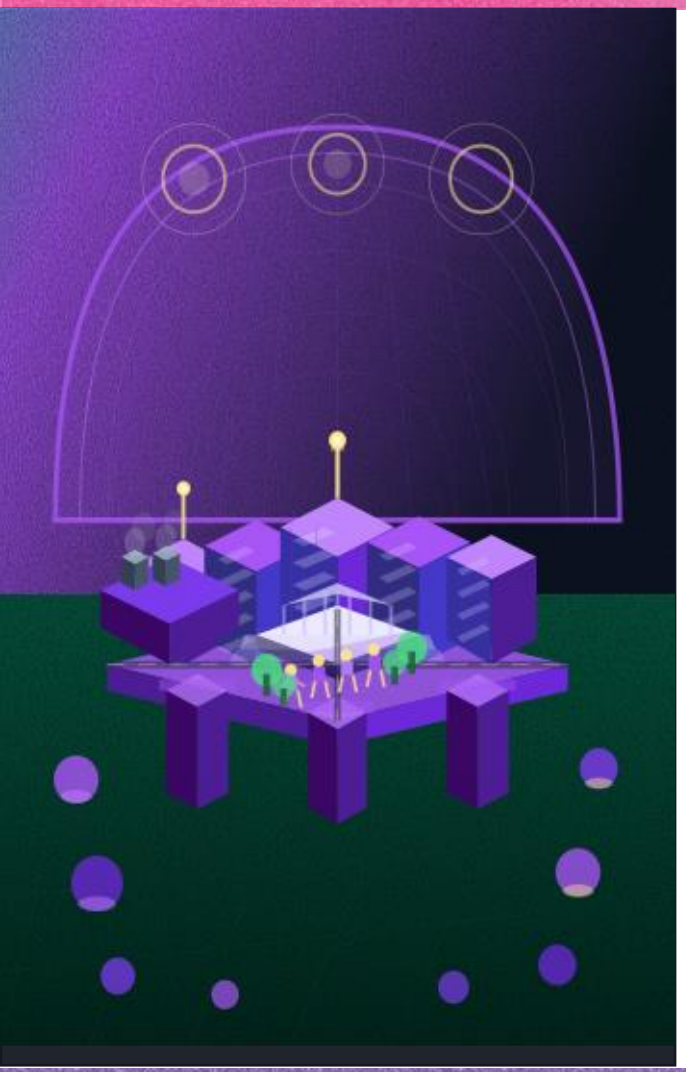
Ausgangslage: Resilienz als strategischer Imperativ

Währenddessen hat der Schweizer Bundesrat in seinem Bericht vom November 2025 digitale Souveränität klar als staatlichen Verantwortungsbereich definiert: Sie beschreibt die erforderliche Kontroll- und Handlungsfähigkeit des Staates im digitalen Raum, um staatliche Aufgaben sicherzustellen. Damit bezieht sich digitale Souveränität klar auf die Verantwortungsbereiche von Verwaltung und Politik. Die Bedeutung von digitaler Souveränität für Unternehmen und die Wirtschaft wird dabei bewusst offengelassen. Die Schweiz stellt damit klar, dass der Hoheitsbereich des Staates nicht in die Verantwortung von privaten Unternehmen und Organisationen eingreift. Umso wichtiger wird nun die Klärung der Folgen, die sich für die Wirtschaft ergeben. Damit verschiebt sich das Thema der digitalen Souveränität von einer operativen auf eine strategische Ebene mit hoher Relevanz für Aufsichtsgremien und Geschäftsleitungen.

In der Konsequenz gilt es nun die konkreten Folgen, Aufgaben und Verantwortungsbereiche für Unternehmen von Konzernen bis KMU zu klären. Voraussetzung ist eine klare Definition der Begrifflichkeiten als Grundlage für die Risikosteuerung und Handlungsfähigkeit in Cloud-, Daten- und KI-Ökosystemen.

Dieses Papier setzt hier an. Es basiert auf einer Grundlagenanalyse des Think Tanks W.I.R.E. in Zusammenarbeit mit Innovate Switzerland aus dem Jahr 2023, einer aktualisierten Analyse der jüngsten Entwicklungen sowie einem vertieften Austausch mit der Community und weiteren relevanten Akteuren im Februar 2026.

Die Voraussetzung liegt in der Klärung der Definition und der Abgrenzung der Begriffe.



2. Definitionen: Drei Ebenen, geteilte Verantwortung

Im ersten Grundlagenpapier von Innovate Switzerland von 2023 wurde digitale Souveränität als «Balance von Freiheit und Kontrolle» im digitalen Raum definiert. In der nächsten Phase der Konkretisierung und Übersetzung in die strategische Planung von Unternehmen braucht es aber eine differenziertere Betrachtung:

Digitale Souveränität, Resilienz und Selbstbestimmung bezeichnen Ziele unterschiedlicher Verantwortungsebenen – nämlich einer staatlichen, einer wirtschaftlichen und einer gesellschaftlichen Verantwortung. Während das übergeordnete Zielbild einer digital handlungsfähigen Schweiz nur durch ein Zusammenwirken aller drei Ebenen erreicht wird, gilt es die Verantwortungs- und Aufgabenbereiche klar zu trennen, um der Komplexität der Thematik gerecht zu werden.

Der Staat schafft den regulatorischen Rahmen auf dem Unternehmen ihre digitale Resilienz aufbauen, um sich so auf die künftigen Anforderungen des Markts und die damit verbundenen Risiken vorbereiten können. Sie tragen durch ihre Robustheit und Handlungsfähigkeit auch zur digitalen Souveränität des Staats als Ganzes bei. Staat und Unternehmen fördern gleichzeitig auch die digitale Selbstbestimmung der Bevölkerung, indem Bürgerinnen und Bürger Wahlmöglichkeiten erhalten digitale Dienste bewusst und informiert zu nutzen.

Erst wenn alle drei Ebenen diese kennen und aufeinander abstimmen, entsteht eine tragfähige digitale Handlungsfähigkeit für die Schweiz. Die drei Verantwortungsebenen sind aber trotz ihrer geteilten Verantwortung klar zu differenzieren:

Die Voraussetzung liegt in der Klärung der Definition und der Abgrenzung der Begriffe.

2. Definitionen: Drei Ebenen, geteilte Verantwortung

Ebene 1: Digitale Souveränität für Staaten

Der Staat verfügt über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum, um staatliche Aufgaben unter allen Umständen sicherzustellen. Dabei werden regulatorische Rahmenbedingungen definiert, die kritische Infrastrukturen schützen. Gleichzeitig stellt der Staat sicher, dass ihn betreffende geopolitische, rechtliche und technologische Abhängigkeiten systematisch erfasst und bewertet werden.

Ebene 2: Digitale Resilienz für Unternehmen

Unternehmen stellen ihre Handlungs- und Wettbewerbsfähigkeit im Rahmen bestehender Abhängigkeitsverhältnisse sicher. Sie können so ihre Zielsetzungen ob in der Produktion oder bei Dienstleistungen stabil verfolgen und bauen aktiv Kompetenzen zur Steuerung ihrer Risikoprofile auf. Resilienz bedeutet in dem Fall nicht, Risiken auszuschliessen, sondern sie zu «managen». Diese Fähigkeit und die Transparenz darüber schafft Vertrauen bei Kunden, Partnern und der Gesellschaft.

Ebene 3: Digitale Selbstbestimmung für die Gesellschaft

Individuen und Bevölkerung behalten die Kontrolle über ihre Daten und ihre digitale Identität, haben Zugang zu digitalen Diensten und Infrastrukturen und verfügen über die Kompetenz, diese mündig zu nutzen. Transparente Wahlmöglichkeiten oder einfache Wechsel zwischen Anbietern schaffen Vertrauen und sind Voraussetzung für die nachhaltige Nutzung digitaler Dienste von öffentlichen und privaten Institutionen.

Die Basis für das Schaffen von Resilienz liegt in der Identifikation von spezifischen Gestaltungsfeldern.

3. Gestaltungsfelder: Checkpoints für digitale Resilienz

Resilienz beschreibt die Fähigkeit einer Organisation oder eines Systems, einer Disruption zu widerstehen, respektive nach einer Krise wieder handlungsfähig zu werden. Um digitale Resilienz in der Realität von Unternehmen zu stärken, gilt es die entsprechenden Herausforderungen und Risiken zu kennen – nur so lassen sich die relevanten Handlungsfelder definieren. Allerdings ist zentral, dass digitale Resilienz nicht durch einzelne Produkte oder Lösungen hergestellt wird, sondern die Fähigkeit definiert, Risiken und ihre Folgen entlang der gesamten Wertschöpfungskette zu kennen und adäquate Strategien zu definieren, wie diese gesteuert werden können. Im Kontext der digitalen Resilienz gilt es für Unternehmen die folgenden Gestaltungsfelder zu bewerten:

1.Strategische Steuerung globaler Lieferketten

Ein gezieltes Management globaler Lieferketten ermöglicht Unternehmen, ihre digitale Infrastruktur nachhaltig und widerstandsfähig zu gestalten. Durch eine vorausschauende Diversifizierung von Bezugsquellen für essenzielle Komponenten wie Chips, Speicher, Energie oder Netzhardware können potenzielle Unterbrechungen – etwa durch geopolitische Entwicklungen oder Engpässe bei Produktionskapazitäten – frühzeitig erkannt und abgefedert werden. So wird die Versorgungssicherheit erhöht und die Grundlage für ein stabiles digitales Ökosystem geschaffen.

2. Vertrauenswürdiger Umgang mit Daten

Unternehmen, die klare Standards für Datenlokalisierung, Zugriffsrechte und Rechtsrahmen setzen, sichern sich langfristig die Kontrolle über ihre sensiblen Informationen, insbesondere im Umgang mit personenbezogenen Daten. Durch den gezielten Einsatz moderner Sicherheitslösungen und den verantwortungsvollen Umgang mit neuen Technologien wie künstlicher Intelligenz lassen sich potenzielle Cyberbedrohungen wie Ransomware oder Phishing frühzeitig erkennen und wirksam abwehren.

Die Basis für das Schaffen von Resilienz liegt in der Identifikation von spezifischen Gestaltungsfeldern.

3. Gestaltungsfelder: Checkpoints für digitale Resilienz

3. Interoperabilität sicherstellen

Die Fähigkeit, Daten sicher und nahtlos zwischen verschiedenen Systemen und Anbietern zu übertragen, ist ein zentraler Baustein für digitale Resilienz. Standardisierte Schnittstellen, die eine reibungslose Kommunikation zwischen Systemen auch in Krisensituationen erlauben, sind ein entscheidender Faktor zur Minimierung von Cyberrisiken und Aufrechterhaltung des Geschäftsbetriebs.

4. Gestaltungsfreiheit und strategische Vielfalt durch ausgewogene Plattformwahl

Unternehmen, die ihre digitalen Dienstleistungen auf eine vielfältige Anbieterlandschaft setzen, erhalten sich maximale Flexibilität bei der Gestaltung ihrer Produkte und Preisstrategien. Durch Diversifikation ihrer Beschaffungsstrategien können Organisationen ihre Handlungsoptionen erhalten und gleichzeitig sicherstellen, dass sie jederzeit auf die für sie passendsten Lösungen zugreifen können. Eine ausgewogene Plattformstrategie unterstützt zudem die Kontrolle über die eingesetzten digitalen Lösungen und damit die Resilienz.

5. Vertrauen und Stabilität durch Einsatz robuster KI-Systeme

Robuste KI-Systeme entstehen nicht durch Technologie allein, sondern durch klare Governance: definierte Regeln, kohärente Prozesse und gezielte Kompetenzentwicklung. Wo diese Voraussetzungen erfüllt sind, liefern KI-gestützte Abläufe zuverlässige Outputs und Prozesse bleiben auch bei Systemausfällen betriebsfähig. Beides stärkt das Vertrauen gegenüber allen Stakeholdern.

Die Basis für das Schaffen von Resilienz liegt in der Identifikation von spezifischen Gestaltungsfeldern.

3. Gestaltungsfelder: Checkpoints für digitale Resilienz

6. Zugangsrestriktionen durch Regulierung

Mit der Zunahme von Regulierungen für digitale Leistungen und KI entstehen geografisch unterschiedliche Restriktionen und generell eine höhere Komplexität für das Betreiben digitaler Lösungen.

7. Transparenter Umgang mit digitalen Identitäten

Digitale Identitäten sind konsistent, eindeutig und systemübergreifend verwaltbar. Einheitliche und klar definierte Zugriffsrechte ermöglichen eine lückenlose Nachvollziehbarkeit und Kontrolle. KI-Agenten werden als digitale Mitarbeitende mit klar zugewiesenen Rollen, Rechten und Verantwortlichkeiten in Unternehmensprozesse integriert, wodurch Sicherheitsrisiken minimiert und die Governance gestärkt werden.

Digitale Resilienz basiert auf vier grundlegenden Voraussetzungen.

4. Grundlagen: Voraussetzungen für digitale Resilienz

Um sich auf die kommenden Herausforderungen vorzubereiten und die Resilienz von Unternehmen zu stärken, gilt es, vier übergeordnete Voraussetzungen zu erfüllen:

1. Betriebsfähigkeit: Rentabilität und Dienstleistungen müssen sowohl bei kurzfristigen Ausfällen einzelner Bestandteile der Wertschöpfungskette funktionieren als auch beim langfristigen Regelbetrieb. Dabei müssen parallel Notfallarchitekturen aufrechterhalten werden, deren Kosten sich in einem adäquaten Verhältnis zu Eintrittswahrscheinlichkeit und Konsequenzen von Risikoereignissen bewegen sollten.

2. Vertrauenswürdigkeit: Unternehmen müssen ihren Kunden stabile Leistungen in konstanter Qualität erbringen können indem sich Daten und Systeme auch unter Druck erwartungskonform und integer nutzen lassen.

3. Schutzwürdigkeit: Kritische «Assets» eines Unternehmens – Daten, Systeme, Infrastruktur – müssen vor externen Zugriffen oder Manipulationen geschützt werden. Da nicht alle Assets gleich exponiert oder geschäftskritisch sind, braucht es eine differenzierte Risikobeurteilung als Grundlage für gezielte Schutzmassnahmen.

4. Steuerbarkeit: Unternehmen müssen in der Lage sein, die zentralen Voraussetzungen für Resilienz adäquat zu kontrollieren. Dies umfasst Exit-Optionen, das Steuern der Risiken sowie Zugang zu der nötigen Infrastruktur und zu Fachkräften.

Die Führungsaufgabe für Unternehmen liegt in der Abwägung zwischen Risiken und Freiheitsgraden und der Einschätzung der Kosten von Resilienz.

4. Grundlagen: Voraussetzungen für digitale Resilienz

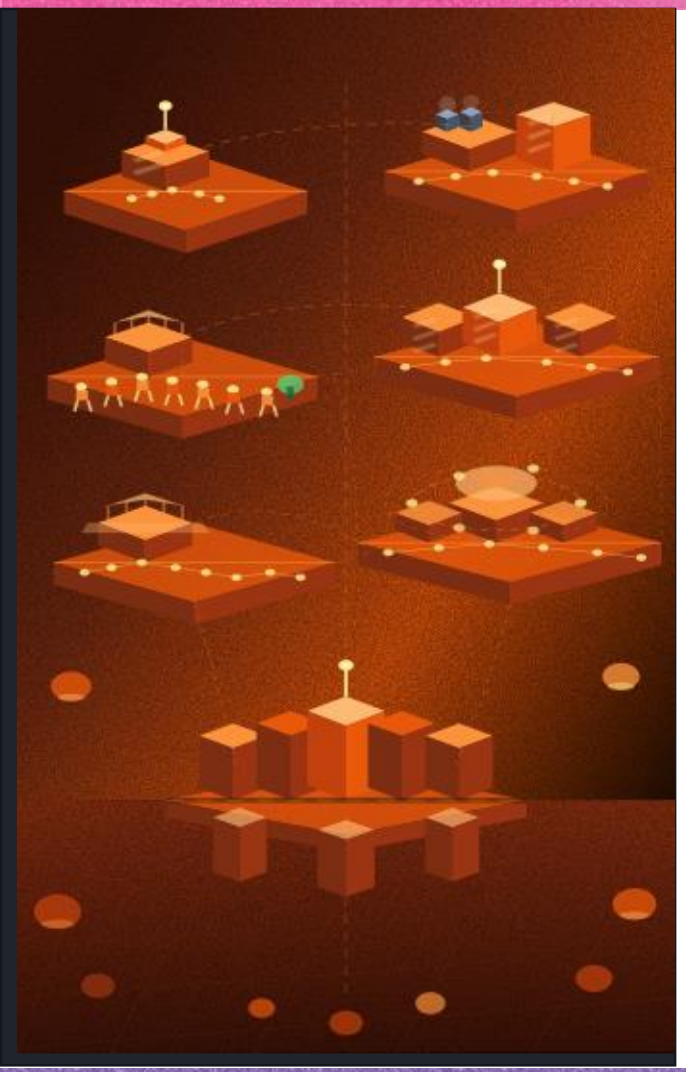
Um ihre Resilienz langfristig zu stärken stehen Unternehmen vor der Anforderung, diese grundlegenden Voraussetzungen entlang ihrer Wertschöpfungskette sicherzustellen.

Für dieses Ziel braucht es einen holistischen Ansatz, bei dem Resilienz nicht als Zustand, sondern als Fähigkeit verstanden wird, die davon ausgeht, dass eine vollständige Entkopplung von allen Risiken nicht realistisch ist.

Resilienz bedeutet, Risikoexpositionen zu kennen sowie Präventions- und verhältnismässige Schutzmassnahmen zu definieren.

Die Führungsaufgabe für strategische Gremien liegt so in der bewussten Abwägung zwischen den Konsequenzen unkontrollierter Abhängigkeit und den Kosten einer überteuerten Redundanz, die kontinuierlich auf neue Bedrohungen ausgerichtet werden muss.

Zum Aufbau von Resilienz gilt es konkrete Handlungsprinzipien und Massnahmen zu definieren.



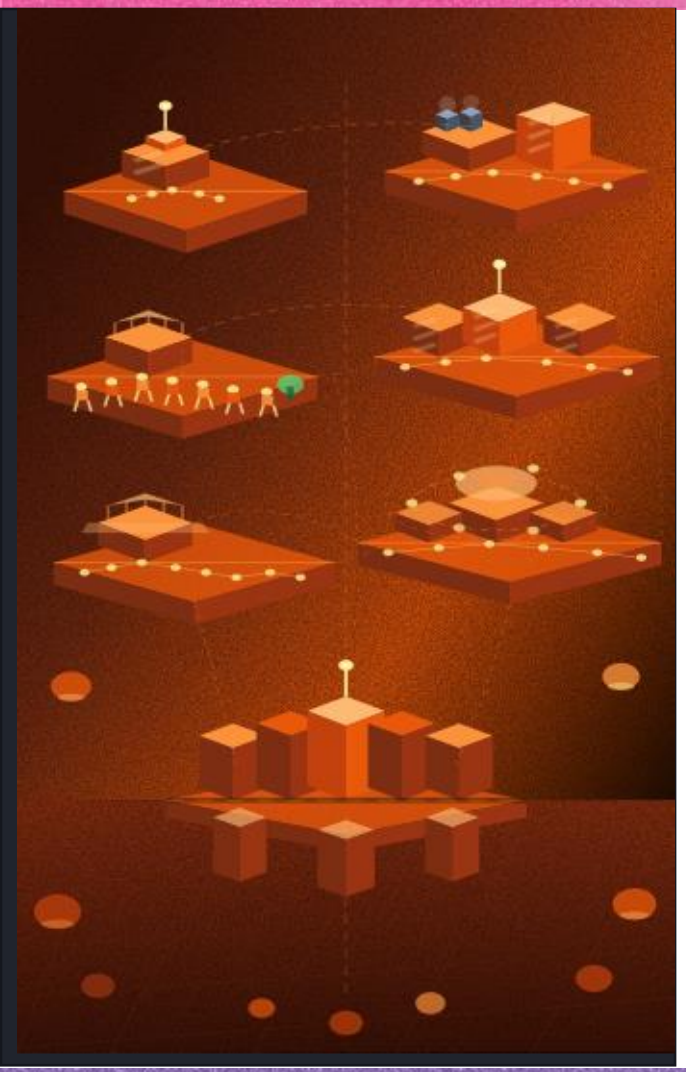
5. Handlungsfelder: Unmittelbare und langfristige Massnahmen zum Aufbau digitaler Resilienz

Der konkrete Weg zur Stärkung der digitalen Resilienz von Unternehmen erfordert ein differenziertes Vorgehen, das unterschiedliche Kompetenzen und Unternehmensbereiche umfasst. Dabei geht es zunächst um das Gesamtverständnis: In einer global vernetzten Welt benötigen Organisationen Zugang zu einem leistungsfähigen Tech-Stack, der Cloud-Lösungen, Microchips bis zu Übertragungsleitungen und Energieversorgung umfasst, ist es weder aus operativen noch aus kostentechnischen Gründen realistisch, eine komplett autonome nationale digitale Infrastruktur aufzubauen.

Mit der zunehmenden Sensibilisierung für Sicherheit, Stabilität und Unabhängigkeit entstehen aktuell in vielen Ländern neue Ökosysteme bestehend aus: lokalen Infrastrukturen, Open Source-Anwendungen und internationalen Angeboten. Aus diesem Spektrum können die Unternehmen diejenigen Architekturen auswählen, die ihrem spezifischen Bedarf am besten entsprechen. Voraussetzung für diesen Prozess sind Transparenz und freie Wahlmöglicheiten, die im Rahmen des Wettbewerbs zu einer Qualitätssteigerung beitragen.

Gerade weil viele Unternehmen unterschiedliche Anforderungen haben, ist davon auszugehen, dass sie unterschiedliche Angebote kombinieren werden und ihre Resilienz dabei durch Kooperation – nicht durch Entkopplung – stärken. Unternehmen, die global agieren, benötigen Partner, die es ihnen ermöglichen, rund um die Welt mit einheitlichen Lösungen im Markt zu operieren. Gleichzeitig eröffnen regionale Lösungen, bei denen beispielsweise kritische Daten auf lokalen Servern gespeichert werden, ein differenzierteres Marktumfeld.

Zum Aufbau von Resilienz gilt es konkrete Handlungsprinzipien und Massnahmen zu definieren.



5. Handlungsfelder: Unmittelbare und langfristige Massnahmen zum Aufbau digitaler Resilienz

Basierend auf einer holistischen Risikoanalyse können Unternehmen so aus unterschiedlichen Angeboten diejenigen auswählen, die ihren Anforderungen am besten entsprechen. Die Voraussetzung dafür ist Transparenz in Bezug auf Leistungen, Limitationen und Kosten der unterschiedlichen Optionen.

Die Schweiz wird ihre digitale Zukunft darum nicht durch Abschottung sichern, sondern in der Fähigkeit, als offener, spezialisierter und verlässlicher Akteur in globalen digitalen Architekturen zu agieren. Interoperable Lösungen und weitere Ansätze, die es ermöglichen, Abhängigkeiten zu kontrollieren, erfordern eine aktive Teilhabe an offenen und globalen Standards. Dies ist nicht nur die Grundlage für das Stärken der Resilienz von Unternehmen, sondern eine mögliche Vision für die Positionierung der digitalen Schweiz im internationalen Marktumfeld als Standort und Kompetenzzentrum für das Verknüpfen unterschiedlicher Angebote, die im Gesamtbild die digitale Resilienz maximieren.

Die Grundlage für den Aufbau digitaler Resilienz basiert auf sechs Prinzipien.

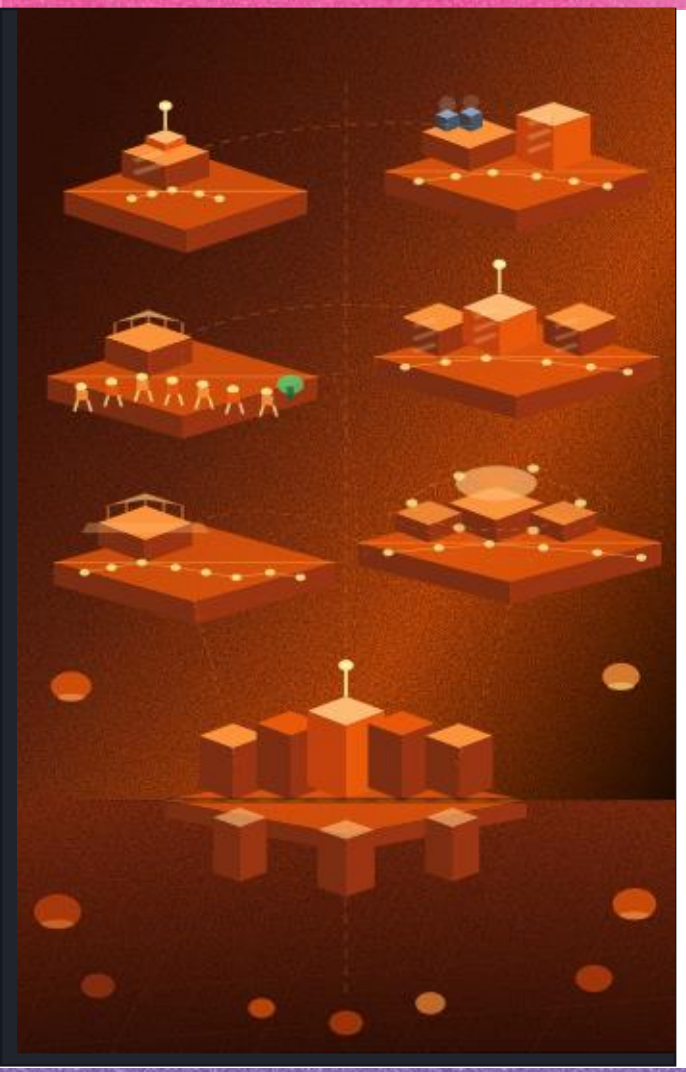
1. Geschäftskritikalität vor Technologiepräferenz

Risikoentscheidungen orientieren sich an der Relevanz eines Angebots für die eigene Wertschöpfung. Je nach Art der benötigten Infrastruktur oder Dienstleistung und dem spezifischen Risikoprofil können lokale oder internationale Anbieter einzeln oder kombiniert genutzt werden. Priorität hat der Schutz des künftigen Systemkerns einer Unternehmung.

2. Steuerungsfähigkeit vor Herkunftslabel

Nicht geografische Herkunft oder technologisches Label entscheiden über Resilienz, sondern ob eine Abhängigkeit aktiv gesteuert werden kann. Nationale Clouds oder Open-Source-Lösungen können Teil einer Strategie sein. Allerdings gilt es abzuwägen, ob diese mit höheren Kosten, Ausfall- und Qualitätsrisiken sowie Kompetenzanforderungen für den eigenverantwortlichen Betrieb verbunden sein könnten.

Zum Aufbau von Resilienz gilt es konkrete Handlungsprinzipien und Massnahmen zu definieren.



3. Bewusste Abhängigkeiten vor maximaler Entkopplung

Da eine vollständige Unabhängigkeit in den wenigsten Fällen möglich und sinnvoll ist, gilt es zu definieren, welche Abhängigkeiten unter welchen Bedingungen akzeptiert werden können. Für den Entscheid über den Schutzgrad von Unternehmensbereichen braucht es eine explizite Positionierung im Spannungsfeld zwischen Kontrolle und akzeptierter Verletzbarkeit.

4. Kompetenz vor Verträgen

Formale Exit-Klauseln aus Verträgen oder der Betrieb redundanter Strukturen schaffen nicht per se Resilienz. Voraussetzung ist eine operative Umsetzungs- und Betriebskompetenz für die gewählte Lösungsarchitektur. Und auch dabei gilt, nicht ein einzelnes Produkt führt zu Resilienz, sondern der kompetente Umgang mit Risikoprofilen und ein Kompetenzaufbau parallel zu technischen Absicherungsmassnahmen.

5. Führung vor Delegation

Die Beurteilung von Risikoexpositionen und den möglichen Folgen von Risiken für kritische Bestandteile der Wertschöpfungskette eines Unternehmens ist Aufgabe von strategischen Gremien. Eine pauschale Delegation an IT-Abteilungen birgt die Gefahr, dass mögliche Folgen für das Geschäftsmodell oder die Reputation übersehen werden.

6. Alternativen vor Standardisierung

Im aktuellen Marktumfeld entstehen neue Geschäftsfelder, bei denen sich die Schweiz international positionieren kann. Die Grundlage dafür sind nicht primär politische, sondern unternehmerische Initiativen. Das Verbinden von Lösungen, die einerseits eine sichere lokale Speicherung kritischer Daten in der politisch neutralen Schweiz mit einer globalen Anbindung ermöglichen, ist nur eines von vielen Beispielen.

Innovate Switzerland legt den Grundstein für wirkungsvolle und nachhaltige Innovationen im digitalen Zeitalter. Die Community entwickelt fundierte und praxisorientierte Thought-Leadership-Inhalte für Entscheidungsträger in Wirtschaft, Politik und Gesellschaft. Im Zentrum steht die Überzeugung, dass ein verantwortungsvoller Umgang mit Cloud und KI-Technologien den Erfolg der Schweiz nachhaltig sichern kann.

Die Community wurde durch den Think Tank W.I.R.E. gemeinsam mit Microsoft initiiert.

Riccardo Merluzzi, Co-Lead Innovate Switzerland

Stephan Pabst, Co-Lead Innovate Switzerland

Dr. Stephan Sigrist, Leiter Think Tank W.I.R.E.

W.I.R.E.

INNOVATE SWITZERLAND