Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

03. Juli 2025

Ergebnisbericht zu den Workshops «Die wichtigsten digitalen Daten der Schweiz»

Inhalt

1 Einleitung 3

2 Zusammenfassung der Ergebnisse der Workshops aus der Perspektive des «Center for Digital Trust» der EPFL 4

3 Zusammenfassung der Ergebnisse der Workshops 2 und 3 aus der Perspektive der «Swiss Data Alliance» 8

4 Dokumentation der Workshops 2 und 3 der «Expedition Zukunft» 11

1 Einleitung

Das Bundesamt für Cybersicherheit (BACS) erarbeitet derzeit Grundlagen zur Umsetzung der Motion 23.3002 «Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz». Die Motion verlangt, dass die bedeutendsten digitalen Daten des Bundes, der Kantone, der Gemeinden sowie der Betreiberinnen kritischer Infrastrukturen besonders geschützt werden. Dazu sollen Kriterien festgelegt werden, anhand deren bestimmt werden kann, welche Daten einem besonderen digitalen Schutz unterstehen, dann soll definiert werden, welche Normen für das Management der Sicherheit dieser Daten gelten sollen und schliesslich soll die Gestaltung der Speicherinfrastruktur für diese Daten nach Möglichkeit Schweizer Organisationen anvertraut werden.

Eine zentrale Herausforderung bei der Umsetzung der Motion ist die Identifikation der wichtigsten Daten der Schweiz. Welche Daten sind für das Funktionieren der Wirtschaft, für das Wohlergehen der Bevölkerung und nicht zuletzt für die Sicherheit der Schweiz unerlässlich? Um mehr Klarheit über diese Frage zu gewinnen, hat das BACS zwischen dem Mai 2024 und Januar 2025 drei Workshops mit Vertreterinnen und Vertretern kritischer Infrastrukturen durchgeführt. Organisiert wurden die Workshops vom «Center for Digital Trust» der EPFL (Workshop 1) und von der «Swiss Data Alliance» in Zusammenarbeit mit der «Expedition Zukunft» (Workshops 2 und 3). Die Workshops zielten darauf ab, praxisnahe Erkenntnisse zum Umgang mit besonders schützenswerten digitalen Daten zu gewinnen. Kritische Infrastrukturen sind Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind. Daten, welche für das Funktionieren dieser Infrastrukturen von zentraler Bedeutung sind, sollen als die wichtigsten und besonders zu schützenden Daten der Schweiz betrachtet werden.

Die Workshops basierten auf einem szenariobasierten Ansatz und nahmen als Ausgangslage den hypothetischen, massenhaften Ausfall zentraler IT-Infrastrukturkomponenten. Im Mittelpunkt stand die Frage, welche Daten für die Aufrechterhaltung essenzieller Dienstleistungen unverzichtbar sind. Die Perspektiven reichten dabei von Energie- und Telekommunikationsunternehmen bis hin zu Akteuren aus dem Gesundheitswesen, dem Finanzsektor und der Lebensmittelversorgung. Die Workshops ermöglichten zudem eine differenzierte Betrachtung branchenspezifischer Anforderungen sowie eine Einschätzung bestehender Abhängigkeiten und Interdependenzen.

Der vorliegende Bericht dokumentiert die zentralen Erkenntnisse aus den Workshops. Er besteht aus drei Teilen, welche von den veranstaltenden Organisationen verfasst wurden:

- Zusammenfassung der Ergebnisse der Workshops aus der Perspektive des «Center for Digital Trust» der EPFL
- Zusammenfassung der Ergebnisse der Workshops 2 und 3 aus der Perspektive der «Swiss Data Alliance»
- Dokumentation der Workshops 2 und 3 der «Expedition Zukunft»

Die Dokumentation der Workshops liefert eine Übersicht über die regulatorischen Grundlagen der Betreiberinnen kritischer Infrastrukturen und deren aktuellen Herausforderungen in Bezug auf Datensicherheit und Compliance. Er zeigt auf, welche Daten die Teilnehmenden im zeitlichen Verlauf eines Ausfallszenarios als besonders kritisch identifiziert haben und beleuchtet die sektorenspezifischen Unterschiede in Bezug auf Datenbedarf und Schutzmassnahmen. Darüber hinaus wird aufgezeigt, welche Massnahmen zum Schutz dieser Daten von den Teilnehmenden angeregt wurden.

Die Ergebnisse unterstreichen die Bedeutung eines koordinierten, sektorenübergreifenden Vorgehens. Nur durch klare Vorgaben, institutionalisierte Zusammenarbeit und die Berücksichtigung technischer wie organisatorischer Aspekte kann die digitale Handlungsfähigkeit der Schweiz nachhaltig gesichert werden. Die Resultate der Workshops bilden eine wichtige Grundlage für die Weiterentwicklung möglicher Handlungsoptionen, welche das BACS zur Umsetzung der Motion 23.3002 ausarbeiten wird. Im Zentrum stehen dabei insbesondere sektorenübergreifende Abhängigkeiten, Anforderungen an den sicheren Datenaustausch sowie Ansätze für eine resiliente digitale Infrastruktur.

2 Zusammenfassung der Ergebnisse der Workshops aus der Perspektive des «Center for Digital Trust» der EPFL

Schutz der Daten kritischer Infrastrukturen der Schweiz in der Cloud: Einblicke und Empfehlungen

Dieses Dokument fasst in einer externen Sichtweise die Ergebnisse aus drei Workshops zusammen, welche das Bundesamt für Cybersicherheit (BACS) 2024-2025 durchgeführt hat, um Grundlagen für die weitere Bearbeitung der vom Ständerat in der Sicherheitspolitischen Kommission eingereichten Motion 23.3002 zu entwickeln. Es soll dem BACS und weiteren beteiligten Verwaltungsbehörden eine unabhängige Bewertung der Ergebnisse und Empfehlungen liefern.

Hintergrund

Als Antwort auf die Motion 23.3002 «Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz» organisierte das BACS zusammen mit verschiedenen Partnern drei Workshops, um die Herausforderungen im Zusammenhang mit kritischen Infrastrukturdaten in der Cloud zu behandeln:

1. BACS/C4DT-Roundtable (EPFL, Mai 2024) - Fokus auf den Schutz kritischer Infrastrukturdaten in der Cloud
2. Swiss Data Alliance (SDA) Workshop 2 (23. Januar 2025) - Fokus auf die Sektoren Lebensmittel, Gesundheitswesen, Notfalldienste, Finanzen und Wissenschaft
3. SDA Workshop 3 (16. Januar 2025) - Fokus auf die Sektoren Energie, Transport, Telekommunikation und Wissenschaft

Die beiden letzten Workshops wechselten von einem datenzentrierten Ansatz zu einer dienstleistungsorientierten Perspektive und untersuchten, wie wesentliche Dienste bei IT-Ausfällen aufrechterhalten werden können.

Wichtige Beobachtungen

Die Workshops ergaben, dass die einzelnen Branchen sehr unterschiedlich gut auf IT-Ausfälle vorbereitet sind. Stark beeinflusst wird diese Vorbereitung von der Kritikalität einzelner Dienste innerhalb der Unternehmen.

Ungleichheiten bei der Vorbereitung der Industrie

- Der Energie- und Telekommunikationssektor zeigte sich durch die Einrichtung von Krisenstäben gut vorbereitet.
- Andere Sektoren zeigten einen unterschiedlichen Grad an Bereitschaft und in einigen fehlten formalisierte Reaktionsmechanismen
- Diese Unterschiede verdeutlichen die Notwendigkeit eines branchenübergreifenden Wissensaustauschs und standardisierter Ansätze

Entwicklung des konzeptionellen Rahmens

- Erster Ansatz: direkte Klassifizierung der Daten nach ihrer Kritikalität.
- Ein sich entwickelnder Ansatz: Zuerst werden die wesentlichen Dienste ermittelt, dann wird bestimmt, welche Daten diese Dienste unterstützen
- Die zeitliche Dimension ist entscheidend - die Kritikalität der Daten hängt davon ab, wie lange die Dienste ohne sie funktionieren können.

Herausforderungen in Bezug auf Workshop-Design und Methodik

- Im C4DT-Roundtable erwies sich die direkte Diskussion über eine Klassifizierung kritischer Daten als wenig zielführend
- Der szenariobasierte Ansatz in den SDA-Workshops war nicht spezifisch genug, was zu einer gewissen Verwirrung unter den Teilnehmern führte: Das Szenario war zu allgemein auf allgemeine IT-Dienste ausgerichtet, anstatt speziell auf die Herausforderungen der Cloud-Infrastruktur einzugehen

Wichtigste Ergebnisse

Zeitleiste der kritischen Bedürfnisse von CI-Anbietern nach dem IT-Ausfall

1. Unmittelbare Phase (Minuten bis Stunden)
    - Kommunikationssysteme (Telefonie, E-Mail) haben höchste Priorität
    - Die Kontinuität der Stromversorgung ist für alle anderen Systeme von grundlegender Bedeutung
2. Mittelfristige Phase (Stunden bis Tag)
    - Betriebskontroll- und Logistikdaten werden unverzichtbar
    - Systeme für Lastmanagement, Zeitplanung und Ressourcenzuweisung müssen wiederhergestellt werden
3. Langfristige Phase (über einen Tag hinaus)
    - Wiederherstellung zentraler Datenbanken und Unternehmenssysteme werden kritisch
    - Finanztransaktionssysteme und Kundendatenverwaltung müssen wieder aufgenommen werden

Inter-Industrielle Abhängigkeiten

- Zwischen den Sektoren bestehen kritische Interdependenzen
- Ausfälle in der Energieversorgung oder der Telekommunikation wirken sich schnell auf andere Branchen aus
- Diese Verflechtungen erfordern eine integrierte Planung über die Grenzen der einzelnen Sektoren hinweg

Regulatorische Landschaft

- Uneinheitliche rechtliche Rahmenbedingungen in den einzelnen Sektoren
- Der Bankensektor verfügt über solide Vorschriften, während es in anderen Bereichen an einem klaren Rahmen fehlt
- Die derzeitigen unverbindlichen Empfehlungen sind möglicherweise unzureichend für den Schutz kritischer Betriebsdaten

Empfehlungen

Strategischer Ansatz

1. Einführung eines “Service-First”-Rahmens
    - Wesentliche Dienste müssen identifiziert sein, bevor kritische Daten klassifizieren werden
    - Entwicklung einer standardisierten Methodik für die Abbildung von Abhängigkeiten zwischen Diensten und Daten
2. Implementierung einer risikobasierten Entscheidungsfindung
    - Entwicklung spezifischer Szenarien für Entscheidungsträger, die verschiedene Bedrohungsmodelle berücksichtigen
    - Berücksichtigung sowohl der unmittelbaren betrieblichen Auswirkungen als auch der weiterreichenden Folgen (Ruf, Wirtschaft)

Operative Verbesserungen

1. Einrichtung von Krisenstäben in allen Sektoren
    - Einrichtung einer branchenweiten Arbeitsgruppe, die sich mit bewährten Praktiken des Krisenmanagements befasst
    - Nutzung des vorhandenen Fachwissens aus dem Energie- und Telekommunikationssektor
    - Validierung von Krisenreaktionsverfahren durch Tests verschiedener Szenarien
2. Sensibilisierung und Schulung des Personals priorisieren
    - Entwicklung umfassender Sensibilisierungsprogramme, um sicherzustellen, dass alle Mitarbeiter wichtige Datenprotokolle verstehen
    - Durchführung regelmässiger Schulungen zu manuellen Ausweichverfahren und Offline-Betrieb
    - Erstellung rollenspezifischer Richtlinien für die Aufrechterhaltung des Betriebs bei IT-Störungen
3. Stärkung des Geschäftskontinuitätsmanagements

   - Entwicklung und regelmäßige Erprobung "IT-freier" Betriebsverfahren (erforderlichenfalls Rückgriff auf papiergestützte Systeme)
   - Sicherstellen, dass kritische Funktionen für bestimmte Zeiträume ohne digitale Infrastruktur weiterlaufen können
   - Erstellung von Sicherungskopien der wichtigsten betrieblichen Unterlagen und Verfahren
4. Verbesserung der Zusammenarbeit zwischen den Branchen
   - Entwicklung von Mechanismen für den Wissensaustausch über Sektorgrenzen hinweg
   - Schaffung formalisierter Kanäle für die Notfallkoordination
   - Regelmässige Prüfung der sektorübergreifenden Abhängigkeiten und Reaktionsmöglichkeiten

Regulierungsempfehlungen

1. Umsetzung einer "weichen Regulierung" mit sektorübergreifender Harmonisierung
   - Vermeidung starrer Einheitslösungen
   - Festlegung gemeinsamer Standards bei gleichzeitiger Berücksichtigung der sektorspezifischen Umsetzung
   - Konzentration auf Ergebnisse statt auf vorgeschriebene Methoden
2. Klare Kriterien für kritische Infrastrukturen definieren
   - Bereitstellung präziser Definitionen und Klassifizierungsrahmen
   - Festlegung von spezifischen Merkmalen, die eine Infrastruktur als kritisch einstufen
   - Sicherstellung einer einheitlichen Anwendung in allen Sektoren

Strategie zur Umsetzung

1. Auf bestehenden Fundamenten aufbauen
   - mit etablierten Krisenteams zusammenarbeiten, anstatt parallele Strukturen zu schaffen
   - Validierung der besten Praktiken durch Tests mit mehreren Szenarien:
     - Versagen der zentralen IT-Infrastruktur
     - Zusammenbruch der Elektrizitätsinfrastruktur
     - Unterbrechungen von Cloud-Diensten (sowohl im Ausland als auch in der Schweiz gehostet)
2. Förderung des Wissenstransfers
   - Schaffung strukturierter Programme für weniger vorbereitete Sektoren, um von fortgeschrittenen Sektoren zu lernen
   - Entwicklung branchenspezifischer Umsetzungsleitfäden auf der Grundlage gemeinsamer Grundsätze
   - Einführung regelmäßiger sektorübergreifender Übungen und Bewertungen

Partnerschaft für Zukunftsforschung

Da die Schweiz den Schutz ihrer kritischen digitalen Infrastrukturen und Daten vorantreibt, stehen die EPFL und das Center for Digital Trust (C4DT) als wichtige Partner bereit, um die Cyberresilienz durch technologiegetriebene Lösungen und Zusammenarbeit zu fördern. Als eine der führenden technischen Hochschulen der Schweiz verfügt die EPFL über erstklassiges Fachwissen in der modernen Cybersicherheitsforschung, das auf die individuellen Bedürfnisse der jeweiligen Branche zugeschnitten werden kann. Durch gemeinsame Forschungsinitiativen kann C4DT den Betreibern kritischer Infrastrukturen helfen, die Robustheit ihrer Systeme zu erhöhen, indem es innovative Ansätze für redundante Systeme und dezentrale Datenspeicherarchitekturen entwickelt, die vor zentralen Ausfallpunkten schützen. Ein weiterer möglicher zukünftiger Schritt ist das Überdenken der Cloud-Nutzung angesichts der geopolitischen Lage. Dabei geht es darum, sich auf Szenarien vorzubereiten, in denen ausländische Cloud-Anbieter von ihren Regierungen gezwungen werden könnten, ihren Kunden unerwünschte Bedingungen aufzuerlegen, wie z. B. die Beendigung von Bemühungen um Vielfalt, Gleichberechtigung und Eingliederung, die Einstellung der Forschung zum Klimawandel oder die Umsetzung anderer politisch motivierter Einschränkungen.

Diese Partnerschaft würde die oben beschriebenen regulatorischen und organisatorischen Maßnahmen ergänzen und sicherstellen, dass die Schweiz auch in den kommenden Jahren einen umfassenden, vielschichtigen Ansatz zur Sicherung ihrer wichtigen digitalen Infrastruktur beibehält.

3 Zusammenfassung der Ergebnisse der Workshops 2 und 3 aus der Perspektive der «Swiss Data Alliance»

Die wichtigsten digitalen Daten der Schweiz

Erkenntnisse aus zwei Workshops, welche die Swiss Data Alliance zusammen mit Expedition Zukunft im Auftrag des Bundesamtes für Cyber Sicherheit BACS im Januar 2025 durchgeführt hat

Das Bundesamt für Cybersicherheit BACS erarbeitet die Grundlagen zur Umsetzung der Motion 23.3002 Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz (Motion im Ständerat, Sicherheits-politische Kommission). Nach dieser Motion müssen bei den wichtigsten digitalen Daten des Bundes, der Kantone und der Gemeinden sowie der Betreiberinnen kritischer Infrastrukturen für «mehr Sicherheit» gesorgt werden. Diskutiert werden Konzepte wie «besonderer digitaler Schutz», Regelwerke zur Definition von Sicherheitsvorgaben und die Frage, an wen die Speicherung von wichtigen Daten übertragen werden soll. Es sind Kriterien festzulegen, anhand deren bestimmt werden kann, welche Daten von welchen Behörden (Bund, Kantone und Gemeinden) und Betreiberinnen kritischer Infrastrukturen einem besonderen digitalen Schutz unterstehen. Das BACS plant, dem Bundesrat bis Mitte 2025 möglichen Handlungsoptionen zur Umsetzung der Motion zu unterbreiten.

Das BACS möchte die Motion in engem Austausch mit den Betreiberinnen kritischer Infrastrukturen bearbeiten und hat deshalb die Swiss Data Alliance zusammen mit Expedition Zukunft beauftragt, zwei halbtägige Workshops zum Thema «Die wichtigsten Daten der Schweiz» durchzuführen. Zu diesen Workshops, die im Januar 2025 stattfanden, wurden ca. 20 IT-Verantwortliche kritischer Infrastrukturen eingeladen, u.a. aus den Sektoren Energie, Gesundheit, Verkehr, Kommunikation, Finanzen und Nahrung. In der Annahme, dass sich die Frage nach den «wichtigsten digitalen Daten» nicht allgemein und abstrakt beantworten lässt, wurde für die Vorbereitung und Durchführung der Workshops das Krisenszenario «Massenhafter und weltweiter Ausfall zentraler IT-Infrastrukturkomponenten» (inspiriert durch die Crowdstrike-Panne im Juli 2024) als Kontext festgelegt. Beide Workshops waren inhaltlich und formal identisch aufgebaut und unterschieden sich nur in der Zusammensetzung der Teilnehmenden aus den verschiedenen Sektoren. Alle Teilnehmenden wurden in einem 30-minütigen Telefongespräch auf die Workshops vorbereitet.

Die Teilnehmenden legten im ersten Teil des Workshops dar, wie sich eine solcher Ausfall der IT-Infrastrukturkomponenten je nach Dauer (Minuten, Stunden, Tage nach dem Vorfall) auf ihre Prozesse («Essential Services»), Systeme und Datenbestände auswirken würde und welche Gegenmassnahmen zu welchem Zeitpunkt in ihren Unternehmen dazu vorgesehen sind. Daraus ergaben sich erste szenario- und zeitbasierte Antworten auf die Frage nach den wichtigsten Daten der jeweiligen Betreiberinnen kritischer Infrastrukturen. Im zweiten Teil des Workshops wurden mit Blick auf die Erhaltung resp. Wiederherstellung der Handlungsfähigkeit («Service Continuity Management») unternehmens- und sektorübergreifend Best Practices, Notfallplanungen, Verbesserung technischer Infrastrukturen sowie regulatorische und kooperative Massnahmen diskutiert.

Erwartungsgemäss identifizierten die Teilnehmenden sehr unterschiedliche Datenbestände, welche von einem Ausfall zentraler IT-Infrastrukturkomponenten betroffen wären und die Aufrechterhaltung der Essential Services verunmöglichen würden. Im Schienenverkehr sind das z.B. die sicherheitsrele-

vanten Daten zur Steuerung der Signale und Weichen, auf welche zu keinem Zeitpunkt verzichtet werden kann. Im Nahrungssektor würde ein Ausfall der Zahlungssysteme innert 15 Minuten zur Schliessung der Verkaufslokale führen. Spitäler müssten ohne interne Kontaktdaten und Kommunikationsverbindungen nach kürzester Zeit die Aufnahme neuer Patienten einstellen und könnten die Durchführung von Operationen nicht mehr gewährleisten.

Die Diskussion der Massnahmen, um die Handlungsfähigkeit bei einem Ausfall zentraler IT-Infrastrukturkomponenten zu erhalten resp. wiederherzustellen, hat gezeigt, dass auf Ebene der einzelnen Unternehmen bereits detaillierte Notfallpläne vorhanden oder in Ausarbeitung sind und umfangreiche Back-up Systeme installiert werden oder bereits zur Verfügung stehen. Zwar bestehen zwischen den Sektoren und den einzelnen Betreiberinnen kritischer Infrastrukturen durchaus signifikante Unterschiede in der Ausprägung und im Implementierungsstatus dieser Massnahmen, aber grundsätzlich konnten die Teilnehmenden darlegen, dass sie die Bedrohung durch ein solches Szenario ernst nehmen und sich darauf im Rahmen ihres Unternehmens vorbereiten. Dabei sind sektorspezifische und sektor-übergreifende Richtlinien hilfreich, wie z.B. das Rundschreiben 2023/1 der Eidgenössischen Finanzmarktaufsicht FINMA («Operationelle Risiken und Resilienz – Banken») oder der Minimalstandard zur Verbesserung der IKT-Resilienz des Bundesamtes für wirtschaftliche Landesversorgung (BWL).

Wesentlich kritischer ist allerdings die Vorbereitung auf notwendige datenbasierte Interaktionen zwischen den Betreiberinnen kritischer Infrastrukturen im Krisenfall zu beurteilen. Die gegenseitigen Abhängigkeiten zwischen diesen Unternehmen und insbesondere der Austausch von Daten zur Aufrechterhaltung resp. Wiederherstellung der Essential Services sind wenig analysiert und finden kaum Niederschlag in sektorspezifischen oder sektorübergreifenden Richtlinien und Standards. Eine besondere Rolle spielen dabei die Telekommunikations- und Energieunternehmen, von deren Diensten praktisch alle anderen Betreiberinnen kritischer Infrastrukturen direkt abhängig sind. Die Teilnehmenden der Workshops warnten zwar mehrheitlich vor der Gefahr einer Überregulierung, befürworteten aber technische, organisatorische und allenfalls sogar gesetzliche Massnahmen, um den sicheren Datenaustausch zwischen den Betreibern kritischer Infrastrukturen in Krisensituationen sektorübergreifend zu gewährleisten. Die Umsetzung der Motion 23.3002 kann dazu den notwendigen Anstoss geben.

Die Workshops bestätigten grundsätzlich den Wert eines szenariobasierten Vorgehens, um den Auftrag der Motion zur Festlegung von Kriterien für die Bestimmung der wichtigsten Daten der Schweiz und deren Sicherheit zu erfüllen. Sie zeigten die Vielfalt der Prozesse, Systeme und Datenbestände, welche je nach Art der Krise und Zeitpunkt betroffen sind. Obwohl wünschenswert wird es aber nicht möglich sein, einen abschliessenden Katalog mit den wichtigsten Daten der Schweiz zu erstellen. Die Umsetzung der Motion erfordert vielmehr eine Methodik, mit welcher ausgehend von den priorisierten Gefährdungen szenariobasiert die wichtigsten Datenbedürfnisse der Betreiberinnen kritischer Infrastrukturen erhoben und daraus die Vorgaben zu deren Sicherstellung abgeleitet werden. Im Fokus muss dabei der Datenverkehr zwischen den verantwortlichen Unternehmen sowie der Verwaltungen des Bundes, der Kantone und Gemeinden stehen. Dieser ist nicht nur mit speziell geschützten technischen Kommunikations- und Speicherinfrastrukturen, sondern auch mit Standards, organisatorischen Massnahmen und rechtlichen Grundlagen zu sichern. Zudem ist der Erfahrungsaustausch und die Zusammenarbeit zwischen den Verantwortlichen der kritischen Infrastrukturen und der Verwaltungen auf allen Ebenen zu fördern.

4 Dokumentation der Workshops 2 und 3 der «Expedition Zukunft»

Expedition Zukunft

Swiss Data Alliance

Expedition Zukunft und Swiss Data Alliance
für das Bundesamt für Cybersicherheit BACS

Workshop Bericht: Essential Services und die wichtigsten digitalen Daten der Schweiz

Version 1.0 | April 2025

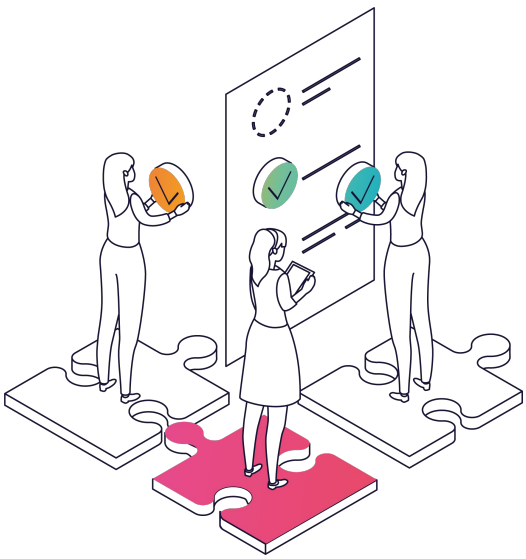
Inhaltsübersicht

Die wichtigsten Daten der Schweiz **S. 3**
- Die Motion 23.3002: Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz..... S. 4
- Ein umfassender Ansatz entlang eines etappierten Vorgehens..... S. 5
- Aufbau und Ablauf der Workshops..... S. 6

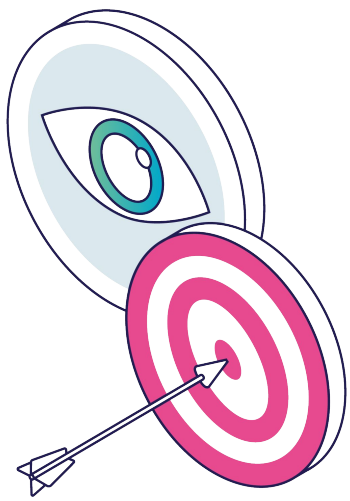
Erkenntnisse aus den beiden Workshops **S. 7**
- Die wichtigsten Erkenntnisse auf einen Blick..... S. 8
- Die wichtigsten Daten entlang der Zeitachse im Szenario..... S. 10
- Die wichtigsten Daten der Betreiber kritischer Infrastruktur..... S. 11

Mögliche Massnahmen und nächste Schritte **S. 12**
- Mögliche Massnahmen: Sicherstellung der zukünftigen Handlungsfähigkeit..... S. 13
- Erkenntnisse zum weiteren Vorgehen..... S. 14

Kontakt S. 15



Die wichtigsten Daten der Schweiz



Die Motion 23.3002: Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz

Mit der parlamentarischen Motion 23.3002 «Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz» ist der Bundesrat beauftragt, die nötigen Rechtsgrundlagen zu schaffen, um bei den wichtigsten digitalen Daten des Bundes, der Kantone und Gemeinden, sowie der Betreiber kritischer Infrastrukturen für mehr Sicherheit zu sorgen.

Die Bundesversammlung – Das Schweizer Parlament
Curia Vista – Die Geschäftsdatenbank

23.3002 Motion

Mehr Sicherheit bei den wichtigsten digitalen Daten der Schweiz

Eingereicht von:	Sicherheitspolitische Kommission SR
Einreichungsdatum:	12.01.2023
Eingereicht im:	Ständerat
Stand der Beratung:	Überwiesen an den Bundesrat

Eingereichter Text

Der Bundesrat wird beauftragt, die nötigen Rechtsgrundlagen zu schaffen, um bei den wichtigsten digitalen Daten des Bundes, der Kantone und Gemeinden, sowie der Betreiber kritischer Infrastrukturen für mehr Sicherheit zu sorgen. Die Vorlage soll insbesondere folgende Massnahmen vorsehen:

1. Es sind Kriterien festzulegen, anhand deren bestimmt werden kann, welche Daten von welchen Behörden (Bund, Kantone und Gemeinden), und Betreibern kritischer Infrastrukturen einem besonderen digitalen Schutz unterstehen.
2. Es ist festzulegen, welche Normen für das Management der Sicherheit dieser Daten gelten sollen.
3. Die Gestaltung der Speicherinfrastruktur ist nach Möglichkeit Schweizer Unternehmen – in Zusammenarbeit mit den Schweizer Hochschulen – anzuvertrauen.

Begründung

.

Stellungnahme des Bundesrates vom 15.02.2023

Die Stärkung der Sicherheit von digitalen Daten und Informationen ist ein wichtiges Anliegen des Bundesrats. Neben dem Datenschutzgesetz (DSG; SR 235.1) enthält insbesondere das in diesem Jahr in Kraft tretende Informationssicherheitsgesetz (ISG; SR 128) Vorgaben zur Klassifizierung und zur Gewährleistung der Sicherheit von Informationen. Die Vorgaben des ISG verpflichten die Kantone jedoch nur dann, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf Informatikmittel des Bundes zugreifen – und keine gleichwertigen Vorschriften haben (Artikel 3 ISG). Für Betreiberinnen kritischer Infrastrukturen, die nicht dem Bund zuzurechnen sind, gelten diese Vorgaben des ISG nicht.

Um den Anliegen der Motion zu entsprechen, ist zu klären, für welche Behörden und Betreiberinnen kritischer Infrastrukturen der Bund die verfassungsrechtliche Kompetenz hat, die geforderten Vorgaben zu erlassen. Der Bundesrat wird dem Parlament für diejenigen Bereiche Vorgaben vorschlagen, in welchen er über die nötigen Kompetenzen verfügt. Für jene Bereiche, in welchen der Bund nicht über die entsprechende Rechtssetzungskompetenz verfügt, wird der Bundesrat Möglichkeiten für das weitere Vorgehen aufzeigen.

Der Bundesrat beantragt die Annahme der Motion.

Antrag des Bundesrates vom 15.02.2023

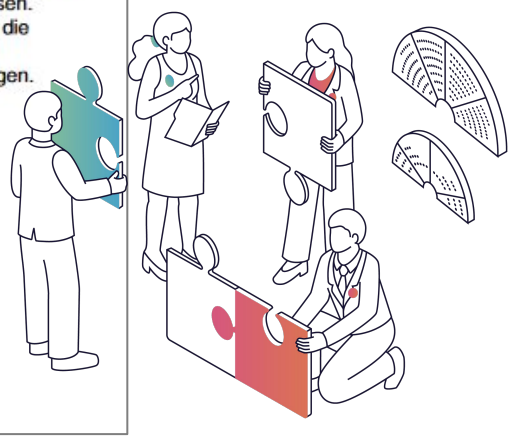
Der Bundesrat beantragt die Annahme der Motion.

Kommissionsberichte

19.06.2023 - Sicherheitspolitische Kommission des Nationalrates

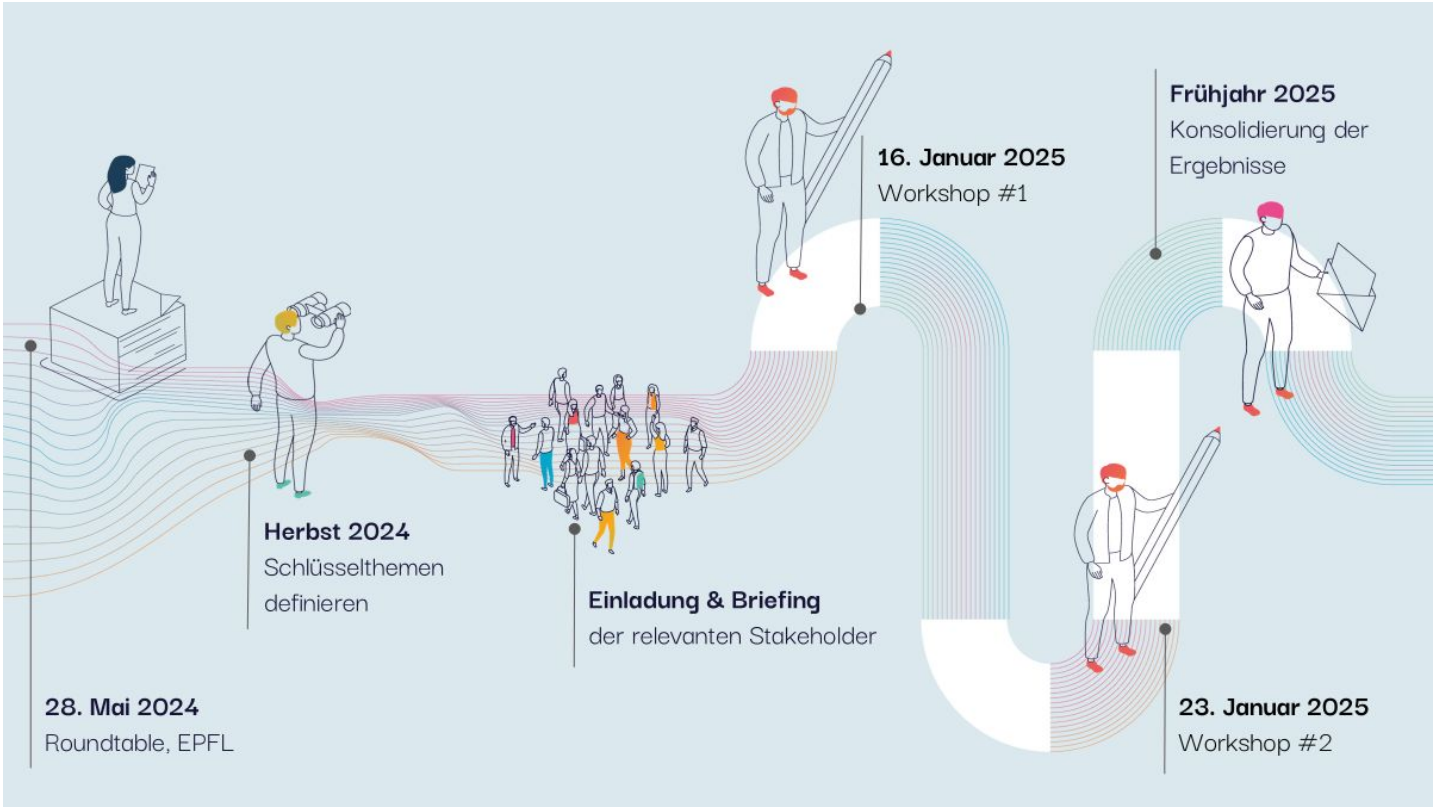
Chronologie

28.02.2023	Ständerat Annahme
19.09.2023	Nationalrat Annahme



Ein umfassender Ansatz entlang eines etappierten Vorgehens

Im Rahmen der Beantwortung der Motion, hat das Bundesamt für Cybersicherheit BACS im Januar 2025 zu zwei umfassenden Workshops zum Thema «Essential Services und die wichtigsten digitalen Daten der Schweiz» eingeladen.



Die Workshops wurden in Partnerschaft mit der Swiss Data Alliance und Expedition Zukunft konzipiert und durchgeführt. Die Workshops sind Teil eines umfassenden Ansatzes, um die Motion szenariobasiert und mit einem kollaborativen Prozess zu adressieren.

Swiss Data Alliance

Expedition Zukunft

Aufbau und Ablauf der Workshops

Im Januar 2025 fanden zwei identisch aufgebaute Workshops für IT- und IT-Sicherheitsverantwortliche von rund 20 Betreibern sogenannter Essential Services in der Schweiz statt. Zu den eingeladenen Branchen gehörten Blaulicht, Energie, Gesundheit, Verkehr, Kommunikation, Finanzen und Lebensmittelversorgung.

Zielsetzung des Workshops

Die Workshops hatten das Ziel, auf Basis der Erfahrungen der teilnehmenden Betreiber grundlegende Massnahmen für mehr Sicherheit der wichtigsten digitalen Daten zu erarbeiten. Die zentrale Fragestellung lautete: «Wie können wir im Kontext eines IT-Ausfalls unsere Handlungsfähigkeit als Betreiber von Essential Services sicherstellen, und wie gewährleisten wir die Verfügbarkeit der dafür notwendigen wichtigsten Daten?»

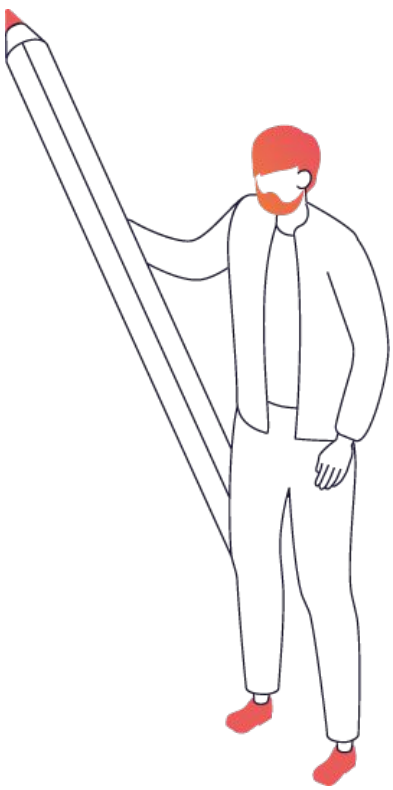
Ablauf und Inhalte

Alle Teilnehmenden der Workshops wurden im Vorfeld durch ein Online-Briefing vorbereitet, um möglichst zielführend am Workshop teilnehmen zu können und ihre Impulse in die legislative Gestaltung einfliessen lassen zu können. Die wertvollen Erfahrungen der Betreiber von Essential Services sollen im Workshop bestmöglich genutzt werden, um Fragestellungen nicht nur aus Unternehmenssicht, sondern auch aus einer nationalen Perspektive zu analysieren.

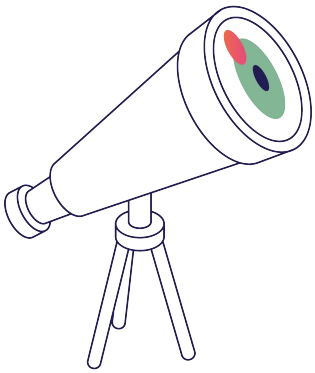
Das Szenario: Ein Massenhafter und weltweiter Ausfall zentraler IT-Infrastrukturkomponenten

Im Rahmen des Workshops wurde ein massenhafter und weltweiter Ausfall zentraler IT-Infrastrukturkomponenten simuliert, ähnlich der CrowdStrike-Panne. Der simulierte Ausfall betraf kritische Systemkomponenten wie Applikations- und Datenbankserver sowie Teile der Cloud-Infrastruktur, wodurch die Nutzung wichtiger Anwendungen und der Zugang zu entscheidenden Daten verhindert wurde. Während des Workshops wurde diskutiert, wie die Wiederherstellung der Handlungsfähigkeit sowie der Schutz der wichtigsten Daten je nach Phase des Szenarios gewährleistet werden kann. Dabei lag ein besonderer Fokus auf der Abhängigkeit von externen Cloud-Anbietern und den Verflechtungen zwischen Unternehmen während der Krise.

Erkenntnisse aus den beiden Workshops



Die wichtigsten Erkenntnisse auf einen Blick



Im Rahmen der Workshops wurden zentrale Erkenntnisse zur Beantwortung der Motion und den geforderten Massnahmen erarbeitet. Die Teilnehmenden entwickelten anhand eines szenariobasierten Vorgehens **1. Kriterien zur Identifikation wichtiger Daten, sowie 2. Normen für das Sicherheitsmanagement dieser Daten.**

Die Gestaltung der Speicherinfrastruktur war dabei nicht explizit Teil der Workshops. Es lässt sich jedoch festhalten, dass die Herkunft der Daten und deren Speicherung, besonders in Cloud-Infrastrukturen, sorgfältig berücksichtigt werden muss, um die Compliance und Sicherheit zu gewährleisten. Die Workshop-Teilnehmenden halten zudem fest, dass ein Verbot der Datenspeicherung im Ausland aktuell erhebliche geschäftliche Einschränkungen nach sich ziehen kann und sorgfältig abgewogen werden muss.

Besonders hervorgehoben wurde das Bedürfnis nach Klärung seitens des Regulators, welche Elemente im Leistungsauftrag kritisch sind und eine Harmonisierung der vorhandenen Vorgaben.

① Festlegung von Kriterien zur Bestimmung wichtiger Daten

Verständnis kritischer Elemente in Leistungsaufträgen: Es ist entscheidend zu definieren, welche Aspekte eines Leistungsauftrags als kritisch betrachtet werden müssen, um darauf basierend adäquate Schutzmassnahmen zu entwickeln.

Branchenspezifische Unterschiede: Es braucht eine Identifizierung und Analyse der spezifischen Anforderungen und Risiken, die sich je nach Branche unterscheiden, um massgeschneiderte Sicherheitsstrategien zu entwickeln.

Interne Branchenunterschiede: Die Workshops führten zur Erkenntnis, dass selbst innerhalb einer Branche signifikante Unterschiede in den Sicherheitsanforderungen und -ressourcen bestehen können für die Aufrechterhaltung der Essential Services.

Szenario und Zeitachse: Die Workshops zeigten deutlich, dass die Kritikalität der Daten stets in Abhängigkeit von einem spezifischen Szenario sowie im zeitlichen Verlauf betrachtet werden muss. Die Festlegung allgemeingültiger – und damit szenario- sowie zeitunabhängiger – Kriterien zur Bestimmung wichtiger Daten gestaltet sich dementsprechend äusserst schwierig.

Datensicherheit und Compliance in der Cloud: Die Herkunft der Daten und deren Speicherung, besonders in Cloud-Infrastrukturen, muss sorgfältig berücksichtigt werden, um Compliance und Sicherheit zu gewährleisten.

Spezifische Strategien für kritische Sektoren: Es müssen spezifische Strategien für kritische Sektoren entwickelt werden, um deren besondere Risiken und Anforderungen zu adressieren.

② Festlegung von Normen bzgl. Sicherheitsmanagement der Daten

Branchen- und organisationsübergreifender Handlungsbedarf: Organisationen sind sowohl innerhalb einer Branche als auch branchenübergreifend Szenario-spezifisch miteinander verflochten und stehen in wechselseitiger Abhängigkeit. Daher besteht ein erheblicher Handlungsbedarf für eine ganzheitliche Betrachtung von Continuity-Management-Massnahmen.

Rolle von Key-Playern: Bestimmte Unternehmen oder Organisationen (z.B. Telekom/Swisscom und Stromversorger) spielen aufgrund ihrer zentralen Position und Vernetzung eine Schlüsselrolle in der Resilienz-Strategie.

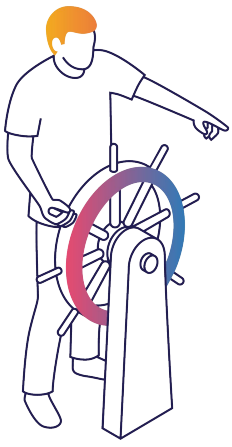
Unterschiedlicher Reifegrad bei Branchenstandards: Der Reifegrad in Bezug auf Standards, Trainings und Know-how im Continuity Management variiert stark – nicht nur zwischen verschiedenen Branchen, sondern auch innerhalb einer Branche zwischen einzelnen Organisationen.

Internationaler Vergleich, besonders Deutschland: Der branchenübergreifende Austausch hat gezeigt, dass einige Organisationen sich an ausländischen Standards und Practices wenden. Es braucht es eine Einbeziehung internationaler Best Practices und Standards, oft genannt wurde Deutschland, zur Verbesserung der nationalen Sicherheitsmassnahmen.

Harmonisierung von Vorgaben: Bereits heute zeigen sich Unterschiede und teilweise auch Widersprüche zwischen verschiedenen Vorgaben, etwa zwischen Branchen sowie auf kantonaler und nationaler Ebene. Die Workshop-Teilnehmenden befürworten daher eine Harmonisierung der Regelungen und Vorhaben.

Verständnis für Interdependenzen: Die Workshops verdeutlichten die Notwendigkeit, branchenübergreifende Vernetzungen besser zu verstehen, um Risiken effektiv zu managen. Diese Erkenntnis ist entscheidend für die Umsetzung der Motion 23.3002 und zielt darauf ab, resiliente Sicherheitsstrategien zu entwickeln, die das Continuity-Management über einzelne Branchen hinweg stärken.

Herausforderungen in der Verfahrensgestaltung: Die Gestaltung und Implementierung effektiver Verfahren stellt eine Herausforderung dar, besonders wenn es um die Sicherheit und Integrität von Daten geht.

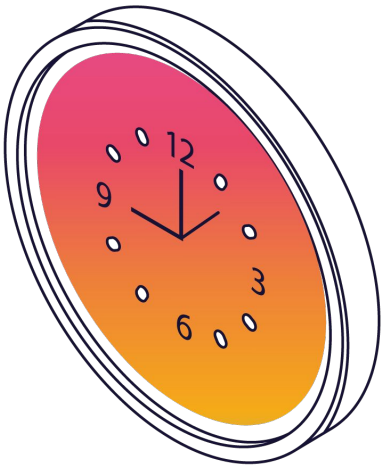


Risikomanagement und Datenspeicherung: Eine umfassende Risikoanalyse ist notwendig, um die Sicherheitsmassnahmen für die Speicherung besonders kritischer Daten festzulegen.

Internationale Vorschriften und geschäftliche Einschränkungen: Ein Verbot der Datenspeicherung im Ausland kann erhebliche geschäftliche Einschränkungen nach sich ziehen und muss sorgfältig abgewogen werden.

Die wichtigsten Daten entlang der Zeitachse im Szenario

Szenariobasiert erläuterten die Teilnehmenden im Workshop, wie sich der Ausfall der IT-Infrastrukturkomponenten im Zeitverlauf – von Sekunden und Minuten bis hin zu Stunden und Tagen nach dem Vorfall – auf die Erbringung ihrer Essential Services sowie auf die betroffenen Systeme und Daten auswirkt. Die Diskussionen zeigten, dass die vorliegenden Ergebnisse jeweils nur im Kontext des gewählten Szenarios betrachtet werden können. Andere Szenarien würden zu unterschiedlichen Ereignisketten führen in den eng verknüpften und miteinander interagierenden Branchen.



Sofortige Reaktionsfähigkeit

Innerhalb der ersten Minuten bis Stunden ist die Verfügbarkeit von Kommunikationssystemen (Telefonie, E-Mail) entscheidend. Dies zeigt die hohe Priorität der Sicherstellung von Kommunikationsinfrastrukturen, um eine sofortige Reaktionsfähigkeit zu gewährleisten. Die Stromversorgung ist essenziell.

Mittelfristige Stabilisierung

Nach einigen Stunden bis zu einem Tag gewinnen Zugänge zu detaillierteren operativen Daten an Bedeutung. Systeme zur Betriebssteuerung und Logistik (z.B. Lademanagement für Fahrzeuge, Disposition von Personal und Fahrzeugen im Schienenverkehr) müssen wiederhergestellt werden, um eine kontinuierliche Versorgung und Mobilität sicherzustellen.

Langfristige Resilienz

Über einen Zeitraum von mehr als einem Tag hinaus wird die Wiederherstellung von Datenbanken und umfassenden Unternehmens-Systemen (z.B. Finanz Transaktionssysteme, Kundendatenverwaltung) kritisch, um die vollständige Geschäftstätigkeit wieder aufzunehmen und rechtliche sowie vertragliche Verpflichtungen einzuhalten.

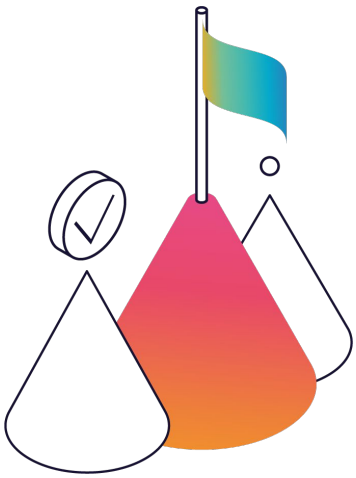
Branchenübergreifende Abhängigkeiten

Die Erkenntnisse zeigen, dass viele Branchen interdependent sind: Ein Ausfall in einem Bereich (insb. Stromversorgung und Telekom) hat sofortige Auswirkungen auf andere Bereiche wie Gesundheitsdienste, Verkehrssysteme oder Lebensmittelversorgung. Dies unterstreicht die Notwendigkeit für integrierte Notfallpläne, die branchenübergreifende Interaktionen und operative Interdependenzen berücksichtigen.

Die Ergebnisse betonen die Bedeutung von robusten Notfallplänen, die nicht nur technische, sondern auch organisatorische Massnahmen umfassen. Dies schliesst die Schulung von Personal, regelmässige Tests der Notfallpläne und die Schaffung von Redundanzen in kritischen Systemen ein.

Die wichtigsten Daten der Betreiber kritischer Infrastruktur

Sektorspezifischer Überblick



Die Diskussionen im Workshop zeigten, dass die verschiedenen Sektoren im Szenario unterschiedlich betroffen sind. Die folgende Übersicht veranschaulicht, welche Daten im gewählten Szenario je Branche besonders betroffen bzw. besonders relevant für die Aufrechterhaltung der Essential Services sind.

Schienenverkehr

- Steuerung des Zugverkehrs: (Signal- und Weichensteuerungen)
- Fahrausweis-Informationen (Verkauf, Kontrolle)
- Wartungsdaten für Rollmaterial (Verfügbarkeit und Status von Zügen)

Luftverkehr

- Passagierinformationen (Check-in, Boarding, Flugstatus)
- Operationsdaten (Flugpläne, Personalzuweisungen)
- Kommunikationssysteme (zwischen Flughafenpersonal und Flugsicherung)

Stromversorgung

- Netzwerksteuerungsdaten (SCADA-Systeme für Energieverteilung)
- Kommunikationsdaten (für Koordination und Notfallmanagement)
- Operative Daten (Energieproduktion, Lastmanagement)

Telekommunikation

- Netzwerkdaten (Betriebsstatus, Auslastung)
- Kundenservicedaten (Kundensupport, Störungsmeldungen)
- Infrastrukturdaten (Status von Datenzentren, Netzwerkknoten)

Finanzen

- Transaktionsdaten (Zahlungsverkehr, Börsenhandel)
- Kundendaten (Kontoinformationen, Transaktionshistorie)
- Systemdaten (Zugriff auf Kernbankensysteme und deren Verfügbarkeit)

Gesundheitswesen

- Patientendaten (medizinische Geschichte, aktueller Status, Behandlungspläne)
- Systeme für Notfallreaktionen (Notrufsysteme, Patientenmanagement)
- Diagnostische Daten (Labordaten, Bildgebung)

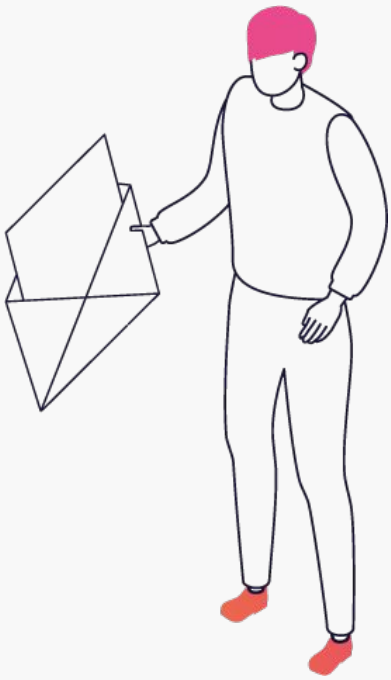
Blaulichtorganisationen (Notdienste)

- Einsatzdaten (Standortdaten, Koordination von Rettungsdiensten)
- Kommunikationsdaten (interne und externe Kommunikationssysteme)

Lebensmittelindustrie

- Liefer- und Logistikdaten (Lieferkettenmanagement, Bestandsdaten)
- Transaktionsdaten (Kassensysteme, Online-Verkauf)
- Warenwirtschaftsdaten (Lagerbestände, Preise)

Mögliche Massnahmen und nächste Schritte



Mögliche Massnahmen: Sicherstellung der zukünftigen Handlungsfähigkeit

Im Workshop diskutierten die verschiedenen Branchenvertreter unternehmens- und sektorübergreifend Best Practices, mögliche Notfallplanungen im Szenario sowie regulatorische und kooperative Massnahmen – stets mit Blick auf die Erhaltung bzw. Wiederherstellung der Handlungsfähigkeit (≪Service Continuity Management≫).

1. Best Practices und Notfallplanung

- **Branchenübergreifende Notfallpläne**: Die Notwendigkeit, robuste und flexible Notfallpläne zu entwickeln, wurde betont. Diese sollten nicht nur technologische, sondern auch organisatorische Aspekte berücksichtigen, um eine schnelle Reaktion auf IT-Ausfälle zu gewährleisten.
- **Redundanzen und Back-ups**: Besonders in kritischen Infrastrukturen – wie der Energieversorgung und im Gesundheitswesen – ist die Implementierung von Redundanzen und regelmässig aktualisierten Back-up-Systemen entscheidend.

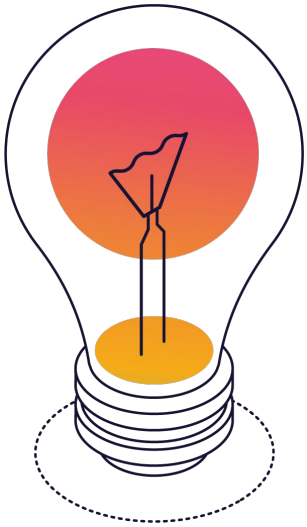
2. Verbesserung der Resilienz durch Technologie

- **Verwendung von fortgeschrittenen Cyber-Sicherheitstools**: Empfehlungen umfassen die Einführung modernster Cyber-Sicherheitsmassnahmen, die speziell auf die jeweiligen Branchenbedürfnisse abgestimmt sind.
- **Erhöhung der Systemrobustheit**: Durch den Einsatz redundanter Systeme und dezentralisierter Datenhaltung soll die Anfälligkeit für zentrale Ausfälle minimiert werden.

3. Regulatorische und kooperative Massnahmen

- **Branchenspezifische Regelungen**: Es wurde vorgeschlagen, spezifische Regelungen zu entwickeln, die die Einzigartigkeit jeder Branche berücksichtigen und klare Vorgaben zur Datensicherheit und -integrität festlegen.
- **Koordination und Zusammenarbeit**: Die Notwendigkeit einer verbesserten Koordination zwischen verschiedenen Branchen und staatlichen Behörden wurde hervorgehoben, um einheitliche Sicherheitsstandards und schnelle Informationsflüsse im Krisenfall zu gewährleisten. Die Interdependenz der Branchen insbesondere im Notfall-Szenario wurde deutlich.
- **Präzisierung durch den Regulator**: Es besteht ein Bedarf an präziseren Definitionen, was unter kritischer Infrastruktur zu verstehen ist. Dies schliesst die Notwendigkeit ein, spezifische Merkmale und Kriterien festzulegen, die eine Infrastruktur als kritisch klassifizieren.
- **Branchenübergreifende Zusammenarbeit und Lernen ermöglichen**: Es braucht Harmonisierung, Förderungen von Best Practices und regulatorische Flexibilität, um gemeinsame Projekte zwischen Sektoren zu erleichtern.

Erkenntnisse zum weiteren Vorgehen



Nach Abschluss der Workshopserie ergeben diverse Erkenntnisse zum weiteren Vorgehen. Die operative Ebene, welche im Workshop repräsentiert war, arbeitet effektiv im Alltag, während die strategische Beteiligung verbessert werden könnte, um eine umfassendere Perspektive zu gewährleisten.

Es ist zudem wichtig zu bewerten, wo der Aufbau oder die Förderung gemeinsamer Infrastrukturen sinnvoll ist, um Synergien zu nutzen und die Resilienz zu stärken. Besonders in der Kommunikation fördern gemeinsame Infrastrukturen die Resilienz im Krisenfall.

Erweiterung der Szenarien: Das szenariobasierte, bottom-up Workshop-Format mit interaktiver Wissenssammlung entlang einer Zeitachse hat sich bewährt, um kritische Daten und Infrastrukturen tiefgreifend zu analysieren. Für ein umfassendes Verständnis ist jedoch die mehrfache Durchführung mit einer Vielzahl von detaillierten und vielfältigen Szenarien notwendig. Auch die Sekundärnutzung von Daten bietet Potenzial, birgt jedoch auch Risiken, die sorgfältig geprüft werden müssen.

Branchenübergreifende Kollaboration: Es besteht ein Bedürfnis zur Schaffung von Plattformen für den branchenübergreifenden Austausch und die Zusammenarbeit, um Synergien zu nutzen und gemeinsame Herausforderungen effektiver zu bewältigen.

Fokus auf Supply Chains: Die Workshop-Teilnehmenden betonten die Notwendigkeit, Supply Chain-Abhängigkeiten zu verstehen und zu managen, statt sich ausschliesslich auf Daten oder deren Speicherorte zu konzentrieren.

Kritische Kommunikation in den ersten Minuten: Die Workshops zeigten die Wichtigkeit einer sofortigen und effektiven Kommunikation unmittelbar nach einem Vorfall und der Verfügbarkeit von Notfallplänen.

Zugang zu Kommunikationssystemen für kritische Infrastrukturen: Branchenübergreifend zeigte sich die Notwendigkeit, kritischen Infrastrukturen einen prioritären Zugang zu robusten Kommunikationssystemen zu gewährleisten, um ihre Funktionsfähigkeit in Krisenzeiten sicherzustellen.

Daten folgen sekundär: Die Workshops zeigten, dass für die Aufrechterhaltung der Essential Services weniger einzelne Daten ausschlaggebend sind, sondern vielmehr die Robustheit der gesamten Supply Chain. Ein besseres Verständnis von Interdependenzen und Ereignisketten in verschiedenen Szenarien kann daher dazu beitragen, kritische Aspekte zur Aufrechterhaltung von Essential Services gezielter zu identifizieren und wirksamer zu schützen.

Regulatorische Anknüpfungspunkte und Anreize: Die regulatorische Strategie kann darin bestehen, an bestehende Meldepflichten anzuknüpfen, um klare Leitplanken dafür zu setzen, welche Leistungen und Verfahren als kritisch gelten. Dies bietet einen Anreiz für Unternehmen, die notwendigen Risikoanalysen durchzuführen und kritische Daten zu identifizieren.

Fall-Back-Optionen: Unternehmen müssen robuste Fall-Back-Optionen entwickeln für den Fall, dass auf externe Daten zugegriffen werden muss, die nicht direkt unter ihrer Kontrolle stehen. So stellen die Unternehmen sicher, dass sie auch bei einem Ausfall externer Datenquellen handlungsfähig bleiben.

Identifizierte Lücken: Die aktuellen gesetzlichen Regelungen decken viele Bereiche ab, jedoch gibt es signifikante Lücken, insbesondere in weniger regulierten Sektoren wie der Lebensmittelbranche. Grosser Bedarf an Harmonisierung der aktuellen Regulierungen und Klärung des Leistungsauftrags von Betreibern kritischer Infrastruktur.

Expedition Zukunft
Gemeinsam mutige Politik designen

Swiss Data Alliance

Expedition Zukunft
Salimata S. Seck
salimata@expeditionzukunft.ch
+41 79 124 32 46
expeditionzukunft.ch

% Impact Hub Bern
Spitalgasse 28
3011 Bern

Swiss Data Alliance
André Golliez, Präsident
golliez@swissdataalliance.ch
+41 79 669 05 52
swissdataalliance.ch

Zurlindenstrasse 111
8003 Zürich