Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

03 juillet 2025

Ateliers sur les données numériques essentielles de la Suisse : rapport

BACS-D-EEFF3401/18

Contenu

1 Introduction 3

2 Synthèse des résultats de l'atelier 1 – Conclusions du *Center for Digital Trust* de l'EPFL 5

3 Synthèse des résultats des ateliers 2 et 3 – Conclusions de la *Swiss Data Alliance* 9

4 Documentation relative aux ateliers 2 et 3 – Expédition Futur (disponible en allemand) 12

1 Introduction

L'Office fédéral de la cybersécurité (OFCS) élabore actuellement les bases légales nécessaires à la mise en œuvre de la motion 23.3002 Pour une meilleure sécurité des données numériques essentielles de la Suisse. Dans celle-ci, la commission de la politique de sécurité du Conseil des États demande que la sécurité des données numériques essentielles de la Confédération, des cantons et des communes, ainsi que des exploitants d'infrastructures critiques, soit augmentée. Elle estime en outre qu'il est nécessaire de fixer des critères permettant de déterminer quelles données doivent bénéficier d'une protection numérique particulière et quelles normes doivent être appliquées pour la gestion de la sécurité de ces informations et, enfin, de recourir, dans la mesure du possible, à des entreprises suisses dans la conception des infrastructures de stockage.

L'un des principaux défis liés à la mise en œuvre de la motion consiste à identifier les données essentielles pour la Suisse : lesquelles sont indispensables au bon fonctionnement de l'économie, au bien-être de la population et, surtout, à la sécurité nationale ? Afin d'apporter une réponse claire à cette problématique, l'OFCS a mené, avec des représentantes et représentants des infrastructures critiques, trois ateliers entre mai 2024 et janvier 2025. Ces ateliers, organisés par le *Center for Digital Trust* de l'EPFL (atelier 1) et par la *Swiss Data Alliance*, en collaboration avec Expédition Futur (ateliers 2 et 3), avaient pour but de rassembler des informations concrètes sur le traitement des données numériques particulièrement sensibles. Les infrastructures critiques sont des processus, systèmes et installations essentiels pour le secteur de l'économie et le bien-être de la population ; les données jouant un rôle central dans le bon fonctionnement de ces infrastructures peuvent donc être considérées comme étant des données numériques essentielles de la Suisse, et bénéficier d'une protection particulière.

Les ateliers étaient fondés sur des scénarios débutant par une panne hypothétique et massive de composants essentiels des infrastructures informatiques ; l'objectif principal était alors de déterminer quelles données sont indispensables au maintien des services essentiels. Des entreprises issues des secteurs de l'énergie et des télécommunications ont pu exposer leur point de vue, de même que des acteurs des domaines de la santé, de la finance et de l'approvisionnement alimentaire. Les ateliers ont également permis d'examiner de manière différenciée les exigences spécifiques à chaque secteur, et d'évaluer les dépendances et interdépendances existantes.

Le présent rapport rassemble les principales conclusions tirées des ateliers. Il se compose de trois parties, rédigées par les organisations responsables.

- Synthèse des résultats de l'atelier 1 – Conclusions du *Center for Digital Trust* de l'EPFL
- Synthèse des résultats des ateliers 2 et 3 – Conclusions de la *Swiss Data Alliance*
- Documentation relative aux ateliers 2 et 3 – Expédition Futur (disponible en allemand)

La documentation relative aux ateliers offre une vue d'ensemble des bases réglementaires devant être respectées par les exploitants d'infrastructures critiques, ainsi que des défis auxquels ces derniers doivent actuellement faire face en matière de sécurité des données et de conformité. Cette documentation présente également les données ayant été identifiées comme particulièrement critiques en cas de panne, et met en lumière les différences entre secteurs des besoins en données et mesures de protection. Elle expose en outre les mesures proposées par les participantes et participants pour protéger ces données.

Les résultats soulignent l'importance d'une approche coordonnée et intersectorielle. En effet, ce n'est qu'à travers des directives claires, une collaboration institutionnalisée et la prise en compte d'aspects techniques et organisationnels que la capacité d'action numérique de la Suisse pourra être garantie sur le long terme.

Les résultats des ateliers constituent une base importante pour l'élaboration de mesures que l'OFCS pourra mettre en œuvre afin de donner suite à la motion 23.3002. L'accent sera notamment mis sur les

dépendances intersectorielles, les exigences en matière de sécurité des échanges de données et les approches visant à garantir la résilience des infrastructures numériques.

2 Synthèse des résultats de l'atelier 1 – Conclusions du *Center for Digital Trust* de l'EPFL

Infrastructures critiques de la Suisse : protection des données dans le cloud
Perspectives et recommandations

Le présent document résume, dans une perspective externe, les résultats de trois ateliers organisés par l'Office fédéral de la cybersécurité (OFCS) entre 2024 et 2025 pour fournir des bases visant à donner suite à la motion 23.3002 déposée par le Conseil des États à travers sa Commission de la politique de sécurité. Il s'agit d'apporter à l'OFCS et à d'autres autorités administratives concernées une évaluation indépendante des résultats et des recommandations.

Présentation

En réponse à la motion 23.3002 « Pour une meilleure sécurité des données numériques essentielles de la Suisse », l'OFCS a organisé trois ateliers avec différents partenaires pour relever les défis liés à la protection des données des infrastructures critiques (IC) dans le cloud :

1. une table ronde OFCS/C4DT (EPFL, mai 2024) centrée sur la protection des données des IC dans le cloud,
2. un atelier Swiss Data Alliance (SDA) (23 janvier 2025) centré sur les secteurs de l'approvisionnement alimentaire, de la santé, des services d'urgence, de la finance et des sciences,
3. un atelier SDA (16 janvier 2025) centré sur les secteurs de l'énergie, des transports, des télécommunications et des sciences.

Ces deux derniers ateliers sont passés d'une approche centrée sur les données à une perspective axée sur les services, en examinant comment maintenir des services essentiels en cas de panne informatique. Les ateliers ont révélé une forte disparité entre secteurs dans le degré de préparation aux pannes informatiques. Celui-ci dépend en grande partie de la criticité de certains des services que leurs entreprises fournissent.

Degré variable de préparation de l'industrie

- Secteur de l'énergie et des télécommunications : bonne préparation grâce à sa capacité à activer des états-majors de crise pour gérer la situation
- Autres secteurs : préparation inégale, certains n'ayant pas encore formalisé de mécanismes de réponse
- Nécessité – mise en lumière par cette disparité – d'échanger des connaissances entre secteurs et d'uniformiser les approches

Développement du cadre conceptuel

- Première approche : classification directe des données en fonction de leur criticité
- Approche adaptative : identification des services essentiels, puis détermination des données indispensables au maintien de ces services
- Dimension temporelle : lien direct entre la durée pendant laquelle les services essentiels peuvent fonctionner sans certaines données et la criticité de celles-ci

Défis relatifs à la conception et à la méthodologie

- Table ronde : discussion directe peu concluante sur la classification des données critiques
- Ateliers : approche par scénario ne répondant pas aux besoins spécifiques, au point d'entraîner une certaine confusion parmi les participantes et participants ; scénario portant sur des services informatiques courants plutôt que d'aborder les défis particuliers posés par l'infrastructure cloud

Résultats principaux

Besoins critiques des exploitants d'IC suite à une panne informatique : chronologie

1. À court terme (entre quelques minutes et quelques heures)
    - Priorité absolue aux systèmes de communication (téléphonie, messagerie)
    - Importance primordiale de la continuité de l'alimentation électrique pour tous les autres systèmes

2. À moyen terme (entre quelques heures et un jour)
    - Préservation indispensable des données logistiques et de contrôle opérationnel
    - Rétablissement des systèmes de gestion de la charge, de planification de la durée et d'attribution des ressources
3. À long terme (au-delà d'un jour)
    - Importance critique de la restauration des bases de données centrales et des systèmes de l'entreprise
    - Reprise des systèmes de transactions financières et de gestion des données clients

Interdépendances

- Interdépendances critiques entre secteurs
- Répercussions sur d'autres secteurs des ruptures d'approvisionnement énergétique ou de télécommunications
- Besoin d'une planification intégrée entre secteurs pour dépasser cette interconnexion

Paysage réglementaire

- Absence d'uniformité juridique entre secteurs
- Absence de cadre clair, sauf dans le secteur bancaire doté de dispositions solides
- Recommandations actuelles non contraignantes et possiblement insuffisantes pour protéger les données critiques

Recommandations

Approche stratégique

1. Prépondérance accordée aux services (*service first*)
    - Identification des services essentiels avant la classification des données critiques
    - Développement d'une méthodologie standard pour illustrer l'interdépendance entre services et données
2. Intégration du risque dans le processus de prise de décision
    - Élaboration de scénarios spécifiques pour les décideurs en tenant compte des différents modèles de menaces
    - Prise en compte des effets immédiats sur l'entreprise et des répercussions plus larges (réputation, économie)

Améliorations opérationnelles

1. Mise en place de cellules de crise dans tous les secteurs
    - Création d'un groupe de travail par secteur sur les bonnes pratiques pour la gestion de crise
    - Recours à l'expertise des secteurs de l'énergie et des télécommunications
    - Validation de procédures de crise en testant différents scénarios
2. Importance de la sensibilisation et de la formation du personnel
    - Élaboration de programmes de sensibilisation aux protocoles de données principaux pour l'ensemble du personnel
    - Mise en place de formations régulières sur les procédures manuelles de secours et de disponibilité hors ligne
    - Élaboration de directives propres à chaque rôle en cas de panne informatique pour le maintien en conditions opérationnelles
3. Renforcement de la gestion de la continuité des activités
    - Développement et mise à l'épreuve régulière de procédures ne recourant pas aux outils informatiques (mais au support papier dans des situations qui l'exigent)
    - Garantie de fonctions critiques sans infrastructure numérique sur une certaine durée
    - Copies de sécurité de la documentation et des procédures principales

4. Amélioration de la coopération entre secteurs
    - Développement de mécanismes de partage des connaissances entre secteurs
    - Création de canaux formalisés pour la coordination des urgences
    - Examen régulier des interdépendances et des possibilités de réaction

Recommandations en matière de régulation

1. Mise en œuvre d'une réglementation souple harmonisée entre secteurs
    - Adoption de solutions uniformisées et modulables
    - Fixation de règles communes intégrant des différences de mise en œuvre entre secteurs
    - Concentration sur les résultats plutôt que sur les méthodes à appliquer
2. Définition de critères clairs pour classer les IC
    - Mise à disposition de définitions précises et de cadres de classification
    - Caractérisation des IC
    - Garantie d'une application uniforme dans tous les secteurs

Stratégie de mise en œuvre

1. Amélioration continue à partir des éléments déjà en place
    - Recours à des équipes de crise établies plutôt qu'à de nouvelles structures redondantes
    - Validation des meilleures pratiques en testant plusieurs scénarios :
        - défaillance de l'infrastructure informatique centrale
        - effondrement de l'infrastructure électrique
        - interruptions des services cloud en Suisse comme à l'étranger

2. Encouragement du transfert de connaissances
    - Création de programmes structurés pour partager les progrès avec les secteurs moins préparés
    - Élaboration de guides pour la mise en œuvre sectorielle sur la base de principes communs
    - Réalisation d'évaluations et d'exercices réguliers pour plusieurs secteurs à la fois

Partenariat pour les études prospectives

L'EPFL et le Center for Digital Trust (C4DT) sont deux importants partenaires qui contribuent à protéger les IC et les données numériques particulièrement sensibles en Suisse et à promouvoir la cyberrésilience grâce à des solutions et une collaboration basées sur la technologie. En tant que haute école technique de pointe, l'EPFL dispose d'une expertise de premier ordre dans la recherche en cybersécurité en vue de proposer des solutions adaptées aux besoins individuels de chaque secteur. À travers des initiatives de recherche conjointes, le C4DT peut aider les exploitants d'IC à améliorer la robustesse de leurs systèmes en développant des approches innovantes pour favoriser la redondance des systèmes et la décentralisation des architectures de stockage de données, ce qui permet de réduire les risques liés aux points de défaillance centraux. L'adaptation de l'utilisation du cloud à la situation géopolitique est une autre étape qui peut être envisagée. Il s'agit de se préparer à des scénarios dans lesquels les fournisseurs étrangers pourraient être contraints par leur gouvernement d'imposer des conditions indésirables à leur clientèle, comme la fin des programmes en matière de diversité, d'égalité et d'inclusion, l'arrêt de la recherche sur le changement climatique ou d'autres restrictions motivées par des considérations politiques.

Un partenariat pour les études prospectives viendrait compléter les mesures d'organisation et de régulation décrites plus haut et garantirait que la Suisse conserve dans les années à venir une approche globale pluridimensionnelle pour sécuriser son infrastructure numérique en fonction de l'importance que celle-ci revêt désormais.

3 Synthèse des résultats des ateliers 2 et 3 – Conclusions de la *Swiss Data Alliance*

Données numériques essentielles de la Suisse

Conclusions tirées de deux ateliers organisés conjointement en janvier 2025 par la *Swiss Data Alliance* et Expedition Futur, sur mandat de l'Office fédéral de la cybersécurité (OFCS)

L'Office fédéral de la cybersécurité (OFCS) est en train d'élaborer les bases légales nécessaires à la mise en œuvre de la motion 23.3002 Pour une meilleure sécurité des données numériques essentielles de la Suisse, déposée au Conseil des États par sa commission de la politique de sécurité (CPS-E). Selon cette commission, la sécurité des principales données numériques de la Confédération, des cantons et des communes, ainsi que des exploitants d'infrastructures critiques, doit être augmentée. La CPS-E aborde également des problématiques telles qu'une protection numérique particulière, des réglementations visant à définir les exigences en matière de sécurité et un transfert de compétence pour le stockage de données importantes. Enfin, elle estime nécessaire d'établir des critères permettant de déterminer quelles données doivent bénéficier d'une protection numérique particulière et quels sont les autorités (fédérales, cantonales et communales) et les exploitants d'infrastructures critiques concernés. L'OFCS entend soumettre au Conseil fédéral, d'ici mi-2025, les options envisageables pour la mise en œuvre de la motion.

Souhaitant travailler en étroite collaboration avec les exploitants d'infrastructures critiques, l'OFCS a chargé la *Swiss Data Alliance* d'organiser, conjointement à Expedition Futur, deux ateliers d'une demi-journée sur le thème « Les données essentielles de la Suisse ». Une vingtaine de responsables informatiques venant d'infrastructures critiques ont été invités à ces ateliers, qui se sont tenus en janvier 2025. Ils représentaient notamment les secteurs de l'énergie, de la santé, des transports, des communications, de la finance et de l'approvisionnement alimentaire. Étant donné que la question des données numériques essentielles ne peut être abordée de façon générale et abstraite, un scénario de crise simulant une panne massive des composants centraux de l'infrastructure informatique à l'échelle mondiale (inspiré de la panne de Crowdstrike en juillet 2024) a servi pour la préparation et la réalisation des ateliers. Les deux ateliers étaient identiques, tant sur le fond que sur la forme, et ne différaient que par la composition des participantes et participants, qui travaillent dans différents secteurs. Un entretien téléphonique individuel de 30 minutes avait été prévu en amont en guise de préparation.

Durant la première partie de l'atelier, les participantes et participants ont exposé les conséquences d'une défaillance des composants de l'infrastructure informatique sur leurs processus (services essentiels), leurs systèmes et leurs bases de données, en fonction de sa durée (minutes, heures, jours après l'incident), avant de présenter les contre-mesures prévues au sein de leurs entreprises respectives, ainsi que le moment envisagé pour leur mise en œuvre. Cela leur a permis d'effectuer une première sélection des données indispensables aux différents exploitants. Dans la deuxième partie de l'atelier, les personnes présentes se sont concentrées sur le maintien ou le rétablissement de la capacité d'action (gestion de la continuité des services). Elles ont donc évalué les bonnes pratiques, les plans d'urgence, l'amélioration des infrastructures techniques, ainsi que les réglementations et mesures de coopérations mises en place aussi bien à l'échelle intersectorielle qu'à l'échelle des entreprises.

Comme attendu, les ensembles de données identifiés comme pouvant être affectés par une panne et, par conséquent, empêcher le maintien des services essentiels, diffèrent fortement en fonction des secteurs. Dans le domaines des transports ferroviaires, les données relatives à la sécurité du contrôle des signaux et des aiguillages sont essentielles et doivent être assurées en tout temps, tandis que, dans le secteur de l'approvisionnement alimentaire, une panne des systèmes de paiement entraînerait la fermeture des points de vente en moins de 15 minutes ; sans données de contact internes ni moyens de communication, les hôpitaux devraient quant à eux cesser rapidement toute nouvelle admission et ne pourraient plus garantir les interventions chirurgicales.

L'analyse des mesures visant à maintenir ou à rétablir la capacité d'action en cas de défaillance de composants centraux de l'infrastructure informatique a montré que des plans d'urgence détaillés existent déjà ou sont en cours d'élaboration dans les différentes entreprises, et que des systèmes de sauvegarde complets sont en cours d'installation, voire déjà disponibles. Bien qu'il existe des différences significatives entre secteurs et entre exploitants en ce qui concerne la nature et l'état de mise en œuvre de ces mesures, les personnes présentes ont généralement montré qu'elles prenaient au sérieux la menace représentée par un tel scénario, et qu'elles s'y préparaient au sein de leur entreprise. À cette fin, elles peuvent s'appuyer sur des directives sectorielles et intersectorielles, telles que la Circulaire 2023/1 de l'Autorité fédérale de surveillance des marchés financiers FINMA (*Risques et résilience opérationnels — banques*) ou la norme minimale pour améliorer la résilience informatique de l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

Toutefois, la gestion, en cas de crise, des interactions nécessaires reposant sur des données entre les exploitants d'infrastructures critiques est dans une situation bien plus préoccupante. Les interdépendances entre ces entreprises et, en particulier, l'échange de données permettant le maintien ou le rétablissement des services essentiels, ont été peu analysés et ne sont guère pris en compte dans les directives et les normes, aussi bien sectorielles qu'intersectorielles. Les entreprises de télécommunications et d'énergie jouent ici un rôle important, car la plupart des autres exploitants d'infrastructures critiques en dépendent directement. Si la majorité des participantes et participants a mis en garde contre le risque de réglementation excessive, elle s'est toutefois prononcée en faveur de l'adoption de mesures techniques, organisationnelles et, le cas échéant, légales. De telles mesures doivent permettre de garantir l'échange sécurisé de données entre les exploitants d'infrastructures critiques dans les situations de crise et ce, pour tous les secteurs ; la mise en œuvre de la motion 23.3002 peut donner l'impulsion nécessaire à cet effet.

Les ateliers ont confirmé qu'une approche basée sur des scénarios était fondamentale pour remplir le mandat de cette motion, à savoir fixer des critères permettant de déterminer quelles sont les données essentielles pour la Suisse et quelles normes doivent être appliquées pour en garantir la sécurité. Ils ont également mis en évidence la diversité des processus, des systèmes et des ensembles de données concernés en fonction du type de crise et du moment où cette dernière survient. Bien que ce soit souhaitable, il ne sera toutefois pas possible d'établir un catalogue exhaustif des données essentielles de la Suisse. La mise en œuvre de la motion nécessite plutôt une méthodologie qui, sur la base des dangers prioritaires et à l'aide de scénarios, permette de recenser les besoins en données les plus importants des exploitants d'infrastructures critiques, puis de déterminer sur cette base les directives permettant de protéger ces données essentielles. L'accent doit être mis sur le trafic de données entre les entreprises responsables et les administrations fédérales, cantonales et communales. Ce dernier ne doit pas être protégé uniquement par des infrastructures de communication et de stockage, mais également par des normes, des mesures organisationnelles et des bases légales. Enfin, il convient d'encourager l'échange d'expériences et la coopération entre les exploitants d'infrastructures critiques et les différentes administrations.

4 Documentation relative aux ateliers 2 et 3 – Expédition Futur (disponible en allemand)

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

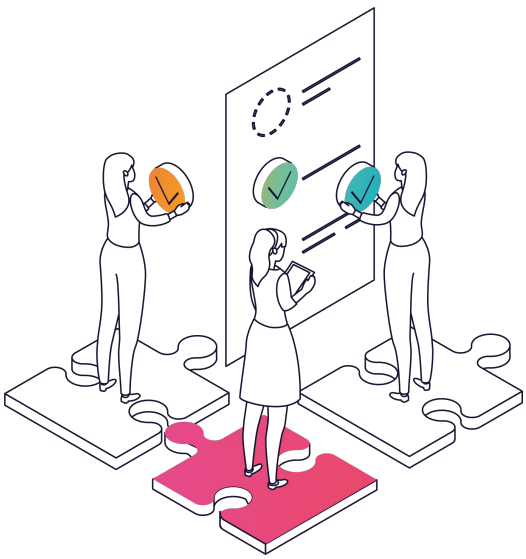
Inhaltsübersicht

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

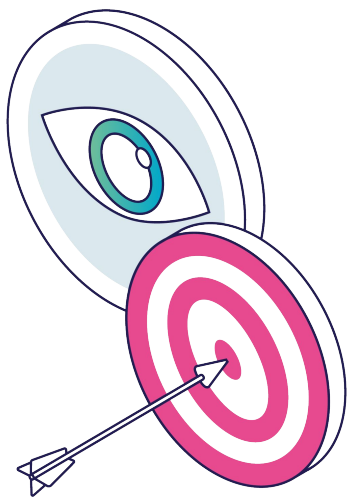
Erkenntnisse aus den beiden Workshops **S. 7**
- Die wichtigsten Erkenntnisse auf einen Blick..... S. 8
- Die wichtigsten Daten entlang der Zeitachse im Szenario..... S. 10
- Die wichtigsten Daten der Betreiber kritischer Infrastruktur..... S. 11

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

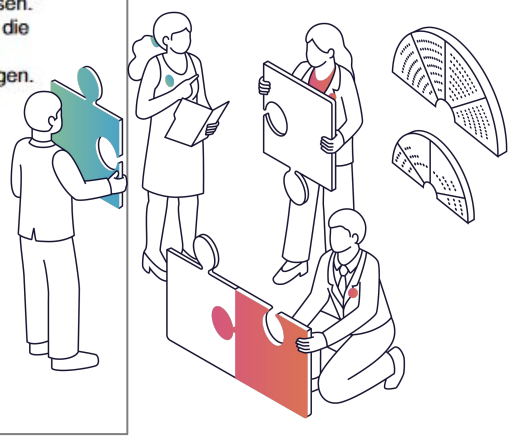
Der Bundesrat beantragt die Annahme der Motion.

Kommissionsberichte

19.06.2023 - Sicherheitspolitische Kommission des Nationalrates

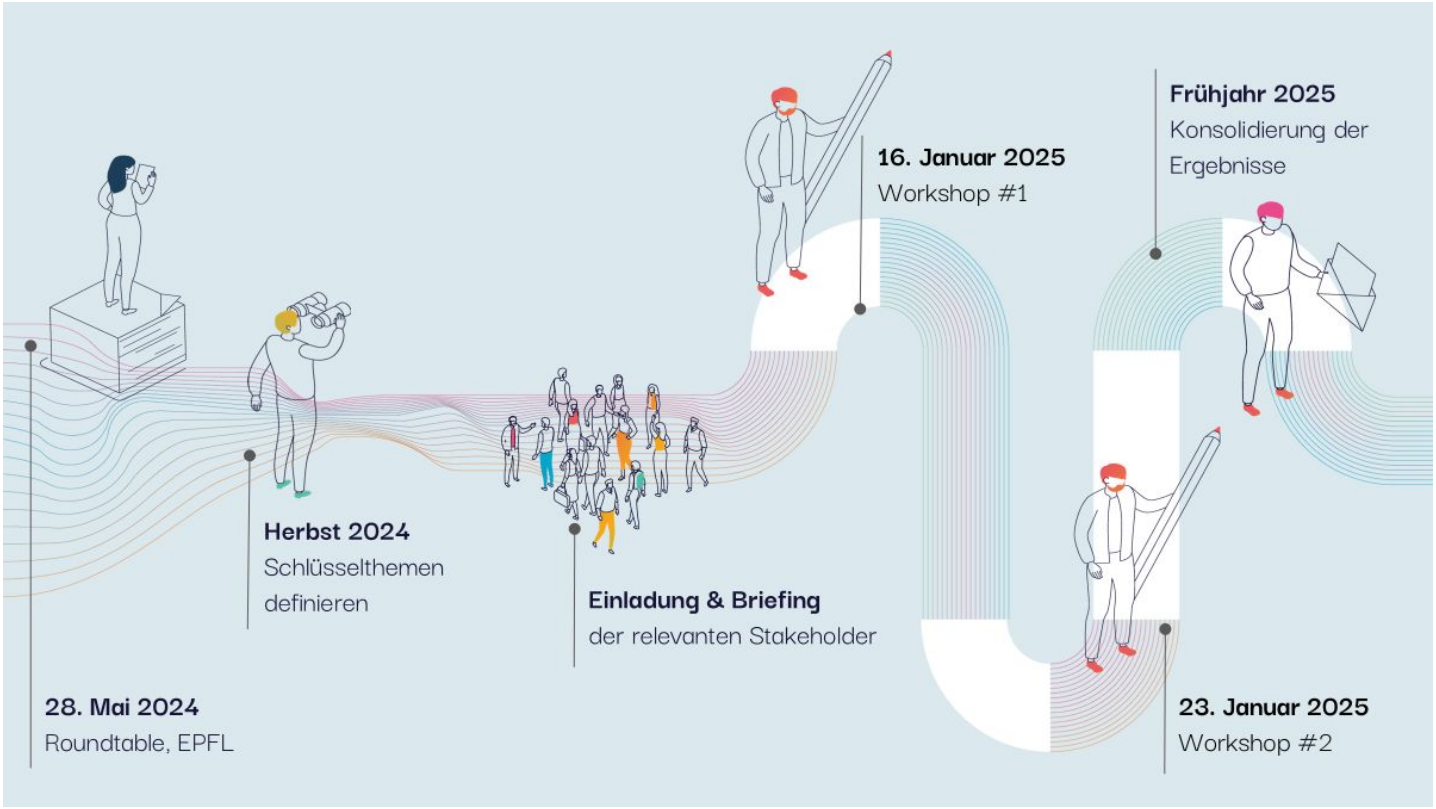
Chronologie

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?»

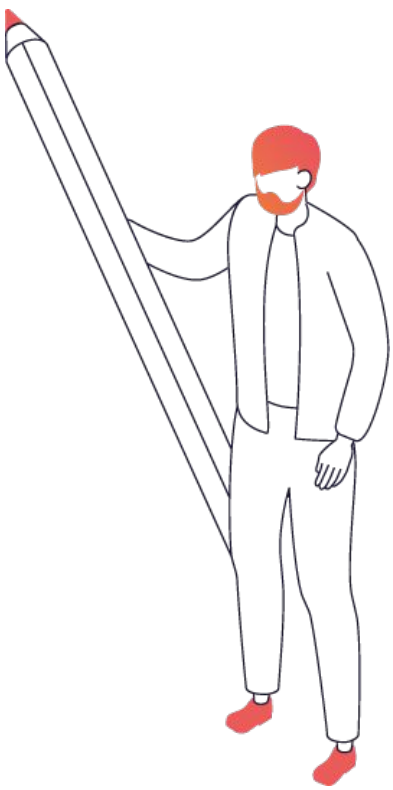
Ablauf und Inhalte

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.

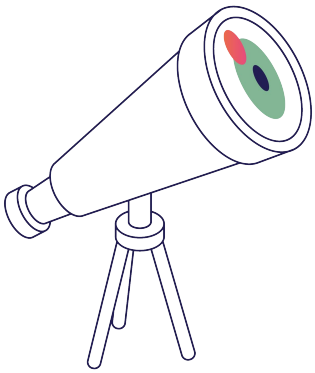
Das Szenario: Ein Massenhafter und weltweiter Ausfall zentraler IT-Infrastrukturkomponenten

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.

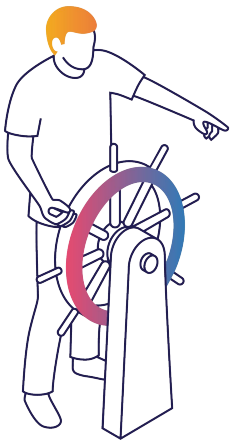
Unterschiedlicher Reifegrad bei Branchenstandards: Der Reifegrad in Bezug auf Standards, Trainings und Know-how im Continuity Management variiert stark – nicht nur zwischen verschiedenen Branchen, sondern auch innerhalb einer Branche zwischen einzelnen Organisationen.

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.

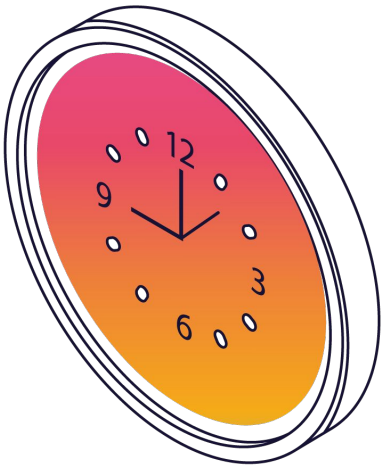


Risikomanagement und Datenspeicherung: Eine umfassende Risikoanalyse ist notwendig, um die Sicherheitsmassnahmen für die Speicherung besonders kritischer Daten festzulegen.

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.

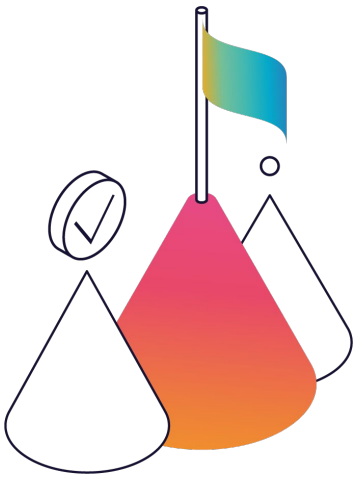
Branchenübergreifende Abhängigkeiten

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)

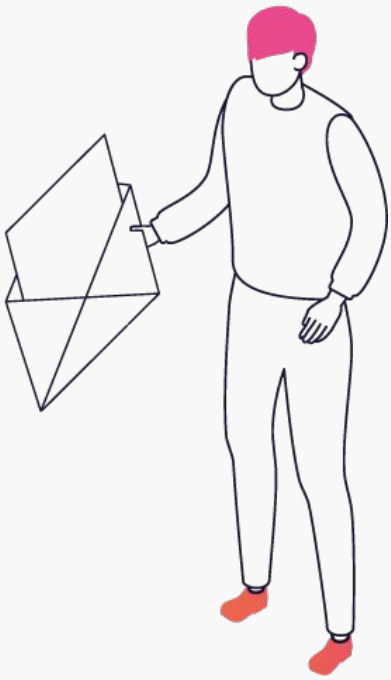
Blaulichtorganisationen (Notdienste)

- 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.

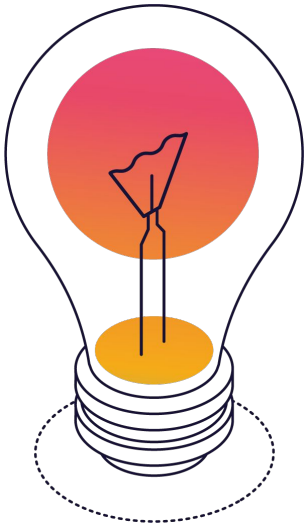
2. Verbesserung der Resilienz durch Technologie

- **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