Resilienzmanagement beim Schutz kritischer Infrastrukturen (SKI) und bei der Nationalen Cyberstrategie (NCS)

Rollen und Aufgaben des BABS

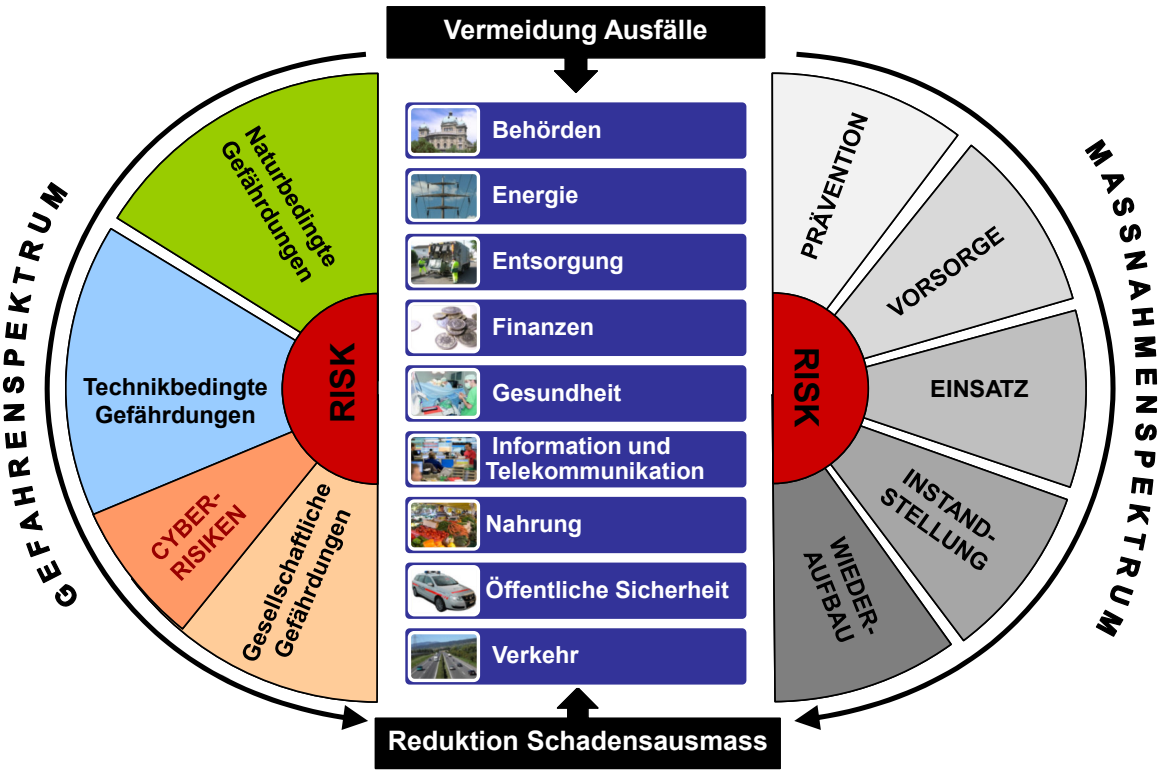
Netclose Community Anlass
HSLU, Rotkreuz, 7. Juni 2023

Dr. Stefan Brem
Chef Weiterentwicklung Bevölkerungsschutz
Bundesamt für Bevölkerungsschutz BABS

Agenda

- **SKI als Konzept – Strategien als Grundlagen**
- **Verbesserung der Resilienz – Resilienzmanagement**
  - Risiko- und Verwundbarkeitsanalyse
  - Resilienzmassnahmen
- **Erkenntnisse**
- **Fragen und Diskussion**

SKI als Konzept: 3 Elemente – 2 Ziele – 1 Ansatz

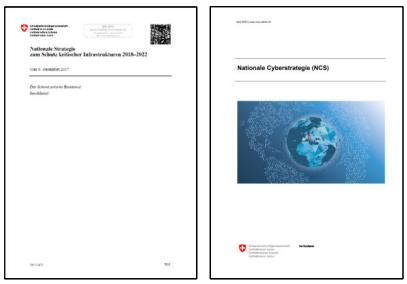


SKI-Strategie und NCS

Abgestimmte Grundlage für die Umsetzung

Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)

Nationale Cyberstrategie (NCS)



Übergeordnetes Ziel

Überprüfung und Verbesserung der Resilienz von kritischen Infrastrukturen in der Schweiz

Handlungsfelder und Massnahmen

- Verbesserung Resilienzmanagement kritische Infrastrukturen
- Standardisierung und Regulierung
- Krisenmanagement / Sensibilisierung

SKI-Strategie und NCS
Gemeinsame Grundsätze

- **Einheitliches Vorgehen** (integraler, risikobasierter Ansatz)
- Verstärkung **öffentlich-private Zusammenarbeit**
- Berücksichtigung **Verhältnismässigkeit**
- **Wahrung** geltender **Zuständig-** und **Verantwortlichkeiten**

17 strategische Massnahmen der SKI-Strategie, u.a.:

- Führung periodisch aktualisiertes Inventar
- Verbesserung Resilienz kritischer Infrastrukturen
- Subsidiäre Unterstützung beim Schutz der KI

SKI-Strategie und NCS
Übersicht Produkte BABS

Nationale Gefährdungsanalyse
Katastrophen & Notlagen Schweiz (KNS)

Schutz kritische Infrastrukturen (SKI)
Beitrag zur Umsetzung NCS

Grundlagen / Vorarbeiten

- Methodenbericht

- Gefährdungskatalog
  44 detaillierte Gefährdungsdossiers

- Risikobericht

Strategie-Umsetzung

- SKI-Inventar (Datenbank)

- SKI-Leitfaden

- **Risiko- und Verwundbarkeits-analysen mit Resilienz-massnahmen**
- **Faktenblätter kritische Teilsektoren**

Verbesserung der Resilienz
Vision und Resilienzbegriff

- **Vision**

  Die Schweiz ist in Bezug auf kritische Infrastrukturen resilient, sodass grossflächige und schwerwiegende Ausfälle möglichst verhindert werden bzw. im Ereignisfall das Schadensausmass möglichst gering gehalten wird.

- **Resilienzbegriff**

  Die Resilienz bezieht sich auf die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen (*Widerstandsfähigkeit*) und die Funktionsfähigkeit möglichst zu erhalten (*Anpassungsfähigkeit*) respektive möglichst schnell und vollständig wiederzuerlangen (*Regenerationsfähigkeit*).

Verbesserung der Resilienz
Top-Down- und Bottom-Up-Ansatz

KI-Betreiber	Fachbehörden, Regulatoren, Branchenverbände
Bereitstellen von Leitfaden, Umsetzungshilfen und Broschüren zur selbstständigen Verbesserung der Resilienz von KI.	**Durchführen von teilsektoriellen Risiko- und Verwundbarkeitsanalysen** zur Identifizierung von systemischen Schwachstellen. Gemeinsames Erarbeiten von **Massnahmen** zur Verbesserung der **Resilienz**.

swissgrid SWISSGAS

Verbesserung der Resilienz
Vorgehensweise und Arbeitsschritte

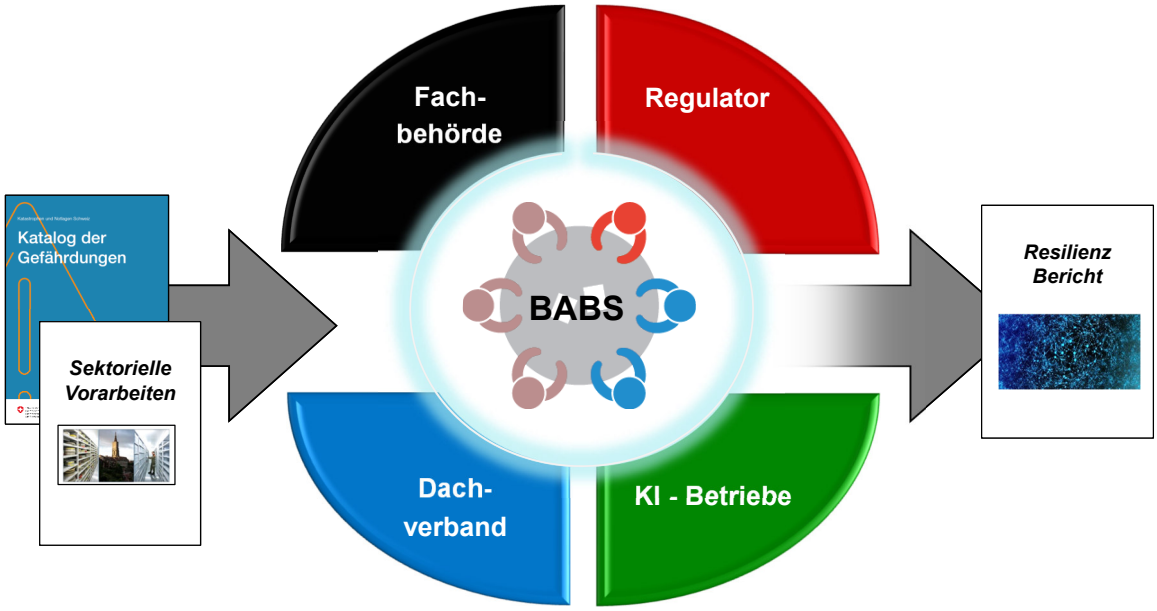
1 System-, Markt-Betrachtung
- Notwendige Versorgungsleistungen bestimmen
- Relevante Akteure, Abläufe, Prozesse und Dienstleistungen identifizieren
- Marktsituation und Rahmenbedingungen bewerten

2 Verwundbarkeitsanalyse
- Kritikalität der Prozesse prüfen
- Abhängigkeit der kritischen Prozesse von Ressourcen prüfen
- Verwundbarkeit der kritischen Prozesse bewerten

3 Risikoanalyse
- Relevante Gefährdungen definieren
- Szenario modellieren
- Eintrittswahrscheinlichkeit bestimmen
- Schadenausmass bei Ausfall der kritischen Prozesse bestimmen

4 Resilienz-Massnahmen
- Mögliche Massnahmen identifizieren
- Kosten-Nutzen Verhältnis bestimmen
- Verantwortlichkeiten für Priorisierung und Umsetzung festlegen

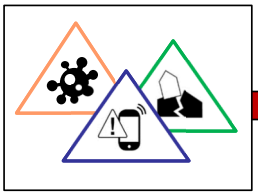
Verbesserung der Resilienz
Involvierte Akteure und Rollen



Risikoanalyse
Vorgehen in vier Schritten

Schritt 1

Gefährdungen



- **Relevante Gefährdungen bestimmen**

Schritt 2

Gefährdungsszenarien

- Beeinträchtigung
- Ausfall
- Zerstörung / Verlust

- **Verifizierung** der **Auswirkungen** des Gefährdungsszenarios auf den Teilsektor und dessen Prozesse
- **Schadensindikatoren festlegen**

Schritt 3

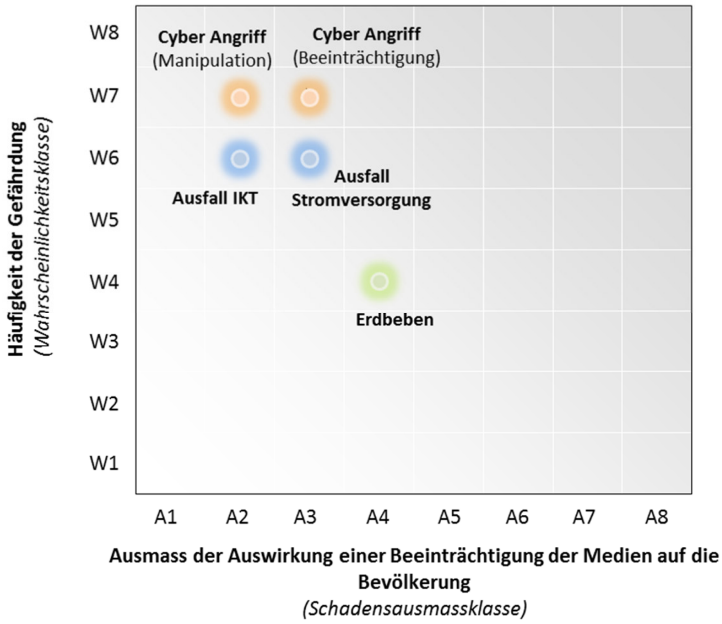
Bevölkerung und Wirtschaft

- Ökonomische Schäden
- Versorgungs-engpässe
- Reputations-/ Vertrauensverlust

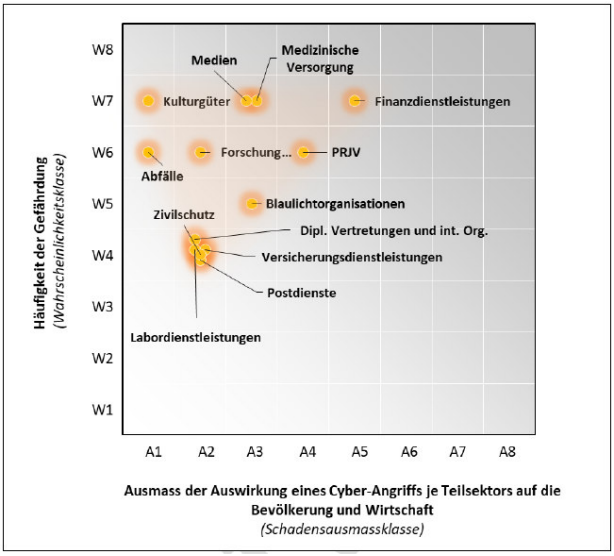
- **Bewerten** des **Schaden-ausmasses** der Beeinträchtigung des Teilsektors/der Prozesse auf die **Bevölkerung** und **Wirtschaft.**

Schritt 4
Zusammenfassung der Ergebnisse

Risikoanalyse
Risikomatrix für kritischen Teilsektor Medien

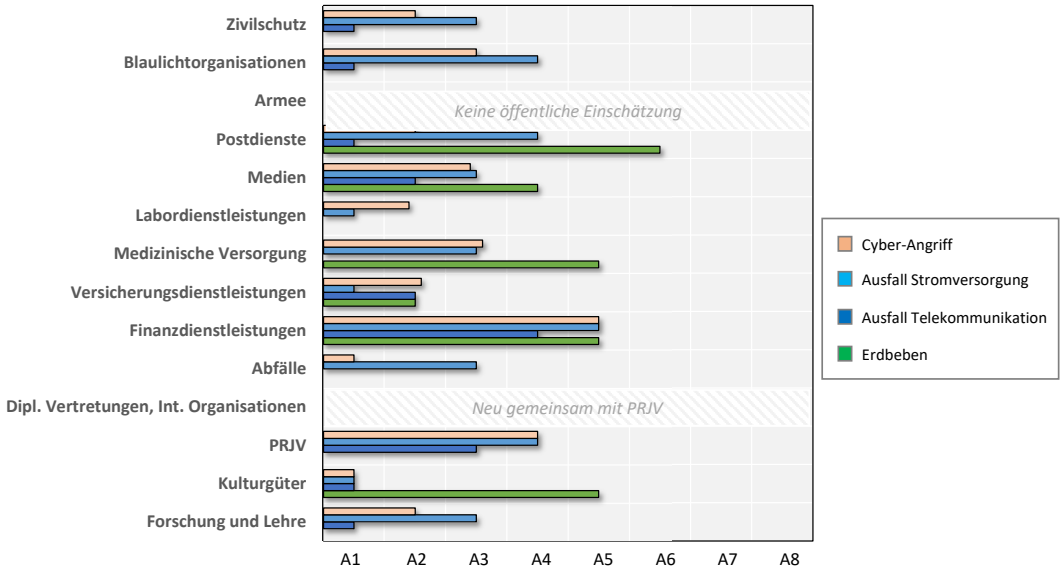


Ergebnisse im Überblick
Risikoeinschätzung Cyber-Angriff



PRJV: Parlament, Regierung, Justiz, Verwaltung

Schadensausmass Gefährdungen
Vergleich des Schadensausmasses durch verschiedene Gefährdungen



Ausmass der Auswirkung verschiedener Gefährdungen je Teilsektor auf die Bevölkerung und Wirtschaft
(Schadensausmassklasse)

* Daten von Dezember 2020

Resilienzmassnahmen
Regulierung / Standardisierung (IKT -> BWL)

Schwachstelle
- Störungen wichtiger Systeme und Anwendungen beeinträchtigen die Erbringung der Leistungen

Massnahme
- Erarbeitung von Empfehlungen / Vorgaben betreffend die IKT-Sicherheit

Ziel der Massnahme
- Verbesserung Widerstands- und Regenerationsfähigkeit von Einrichtungen gegenüber Ausfällen kritischer Systeme/Anwendungen

Resilienzmassnahmen
Schulung und Sensibilisierung (IKT)

Schwachstelle
- Objekte/Prozesse sind angreifbar, da Arbeitskräfte zu wenig mit den Risiken der zunehmenden Digitalisierung und Vernetzung vertraut sind.

Massnahme
- Sensibilisierung der Mitarbeitenden gegenüber Cyber-Risiken und Informations- und Datensicherheit

Ziel der Massnahme
- Verbesserung des Bewusstseins der Fachkräfte gegenüber Cyber-Risiken und der Bedeutung von Datensicherheit

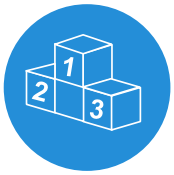
Resilienzmassnahmen
Behördliches Krisenmanagement (übergreifend)

Schwachstelle

- Längerdauernde und grossflächige Ereignisse können die Erbringung von Leistungen auf nationaler Ebene beeinträchtigen.

Massnahme

- Prüfung von Vorgaben zur Priorisierung spezifischer Leistungen während gravierenden Ereignissen



Ziel der Massnahme

- Sicherstellung der lebensnotwendigen Leistungen während gravierenden Ereignissen

Resilienzmassnahmen
Kontinuitäts- und Notfallpläne

Schwachstelle

- Leistungen sind erheblich beeinträchtigt, wenn Lieferanten / Partner ihre Leistungen nicht erbringen oder Produkte nicht liefern können.

Massnahme

- Verbesserung des Umgangs mit Ausfällen oder Beeinträchtigungen von Lieferanten und Partnern durch vordefinierte Abläufe

Ziel der Massnahme

- Verbesserung der Widerstandsfähigkeit von Einrichtungen bei Ausfällen/Störungen von Lieferanten und Partnern

Resilienzmassnahmen
Durchführung/Teilnahme Krisenübungen

Schwachstelle
- Der heutige Stand der Widerstands- und Regenerations-fähigkeit ist nicht ausreichend bekannt.

Massnahme
- Durchführung von branchenweiten bzw. teilsektorübergreifenden Übungen

Ziel der Massnahme
- Training und Sensibilisierung der beteiligten Stellen/Akteure
- Identifikation von Schwachstellen und Stärken

Resilienzmassnahmen
Verbesserung der Vernetzung

Schwachstelle
- Informationen zu Cyber-Angriffen oder zu Störungen werden noch nicht adäquat ausgetauscht.

Massnahme
- Verbesserung des Informations- und Erfahrungsaustauschs zwischen den relevanten Unternehmen / Fachstellen

Ziel der Massnahme
- Schnelle und adäquate Reaktion durch die Organisationen im Falle von Cyber-Angriffen und bei Störungen von Gerätschaften

Erkenntnisse
Risiko- und Verwundbarkeiten

Zunahme übergreifender Risiken und Interdependenzen

(Über-)Regionale Ereignisse (z. B. Blackout) beeinträchtigen die Versorgung mit Leistungen auf nationaler Ebene.

Steigende Abhängigkeit von Informations- und Kommunikations-systemen erhöht Auswirkungen von Unterbrüchen / Vorfällen.

Wichtige Handlungsfelder

- Cyber-Vorfälle und IKT-Ausfälle
- Ausfälle essentieller Güter und Leistungen von Dritten (Lieferketten-Problematik)
- Ausfälle von (Schlüssel-) Personal

Erkenntnisse
Resilienzmassnahmen

Die zunehmende Vernetzung und Digitalisierung schafft vermehrt Angriffsvektoren (Cyber-Angriffe auch über Partner/Lieferanten).

Ein integrales und risikobasiertes Vorgehen für die Identifikation von Schwachstellen und die Reduktion von Risiken ist essentiell.

Dialog und enge Zusammenarbeit zwischen den relevanten Fachstellen sind Schlüsselfaktoren zur Verbesserung der Resilienz.

Krisensituationen lassen sich nicht abschliessend planen. Vorsorgliche Notfallplanungen und Business Continuity Management und insbesondere Übungen sind unerlässlich für eine erfolgreiche Bewältigung von gravierenden Ereignissen.

Fragen und Diskussion

Vielen Dank für die Aufmerksamkeit!

Kontaktadresse

Dr. Stefan Brem
Chef Weiterentwicklung Bevölkerungsschutz
Bundesamt für Bevölkerungsschutz BABS

Guisanplatz 1B, 3003 Bern
Tel +41 58 462 51 37
stefan.brem[at]babs.admin.ch
www.bevoelkerungsschutz.ch

Weiterführende Informationen:
Nationale Risikoanalyse KNS: www.risk-ch.ch
Kantonale Gefährdungsanalyse: www.kataplan.ch
Schutz Kritischer Infrastrukturen SKI: www.infraprotection.ch